電子認証局の法的責任

2002 年 4 月 12 日

弁護士　　牧野　二郎

〒160-0023　　東京都新宿区西新宿 1-13-12　西新宿昭和ビル 9 階
TEL (03)5339-2776　FAX (03)5339-2779

目次

電子認証局の法的責任

牧　野　二　郎

0　はじめに

わが国においても電子署名制度※1 が始まり、電子署名の認証業務を行う複数の特定認証局が実働を始めている。こうした認証業務に関して、認証の持つ効力、誤認証を行った場合の法的責任、損害賠償の関係は必ずしも明確にされていない。電子署名、認証制度が実用化されるのは人類史上初めての経験であり、また、実態としてトラブルが発生し、損害賠償の問題が議論された実例にも乏しく、今後の研究、実践を待つ部分が大きい。

電子署名は、すでに実用化されているが、これをめぐる法的問題はほとんど検討されていないといってよい。電子署名の持つ法的効果、推定力に関してはいくつかの研究もなされているが、トラブルを想定した損害賠償問題については、経済産業省が定めた電子商取引準則が提供されたに過ぎない。同準則では、成りすましに関する契約責任、不法行為責任に関して類型的に検討されてはいるものの、CP・CPS といった認証局の持つルールとの関連は未検討の課題となっている。

電子署名制度が、オンラインでの存在確認、属性確認という困難な課題を克服する制度として提案され、実用化されているのだが、信頼を確保するには多くの経験と慣習がしっかりと確立する必要がある。ここでは、そうした新しい信頼の制度が確立するために必要な適正な責任配分、インフラとしての認証局の負担すべきリスク、利用者の負うべき義務などを検討することにする。

その際、最も参考になるのが印鑑証明制度である。印鑑を登録し、その証明を発行し、その証明書は不動産取引などで重要な役割を果たす。印鑑証明はまた、身分証明ともされるなど、多様な形で社会の信頼を支えるものとなっている。ところが、同時に数百円で発行される唯の登録証明なのだが、数億円の取引の必須の書類とされることで、その登録、発行ミスが招来する損害は膨大なものとなる危険を内包する。しかし、印鑑証明制度はそうした危険性をよそに、淡々と続けられ、市民はこれを貴重な制度として、信頼し利用を続ける。こうした、紙片１枚が持つ信頼は、電子署名とその認証に相通ずるものがあると思われるので、その角度から責任を検討しようと思い立ったのである。

印鑑証明制度は、法律によって定められたものではない。長い歴史の中で、慣習として確立したものであって、それを地方自治体が条例を制定して制度化※2 しているものである。

※1　電子署名と認証業務に関する法律（平成十二年五月三十一日法律第百二号）

※2 「印鑑の登録及び証明に関する事務について」平成１１年１２月２２日改正自治振第　　１７５号　自治省行政局振興課長から各都道府県総務部長宛　住民基本台帳法令・通達集　平成１３年版　ぎょうせい

印鑑証明制度が不動産取引にとどまらず、信頼確保の制度として確固たる地位を占めていることを考えると、国民の信頼を確保する制度であれば、あるいはまた、そうした信頼制度が実用性を備え、信頼の連鎖を確立する仕組みであれば、法律がなくとも強固なインフラとして確立することがわかる。われわれが、電子署名制度をオンラインで機能する信頼の制度にする為には、電子署名とその認証制度による証明があることにより、多くのメリットを享受することができ、相互に信頼することが可能となること、すなわちオンラインでの信頼の連鎖を確立することが重要なのである。

電子署名の法的問題、責任関係を検討するということは、同時に現在の既存の制度を再検討することでもある。改めて検討すると、現行の制度の合理性と、同時に制度としてのおおらかさ、微妙なバランスの上で機能する有様に驚くのである。しかし、それは国民の意識や慣習といったものに支えられ、相当強固な仕組みとして存在していることもまた事実である。ところが、オンラインではそうした慣習が確立していないため、ビジネスをすすめるにはあまりに未完成でありすぎる。従って、われわれは現行制度を検討すると同時に、オンラインでの特性、リアルな世界との差を十分に検討することで、リーズナブルなシステムのあり方、責任分配を提案しなければならない。

この論文では、現在進められている各認証局の責任回避の妥当性を考察し、言及することになる。何らかの参考になれば幸いである。

0-1　検討の対象

現在、おおかたの認証局の認証のシステム構築内容とその運用方法は、RFC2527 をはじめとする一連の関連ＲＦＣに準拠していると見て良い。RFC は、インターネットの規格を確定し、インターネット上の各種のシステムの構築、研究を推進している世界的組織である ISOC（INTERNET　SOCIETY）※1 で議論され、公開された関連提案が、数ヶ月の審理期間を経て RFC（REQUEST　FOR　COMMENT）として確定し、公表される。その他 IETF（The Internet Engineering Task Force）※2 をはじめとする国際的機関で検討された議論を基礎とし、あるいは ABA※3 のルールを基にしている。

RFC2527（Request For Comments 2527）※4 の規定する認証局、公開鍵インフラストラクチャのための認証ポリシーもしくは認証実施規程を作成するためのフレームワークは、認証局の基本的構造、そのガイドラインを提供している。各国認証局は、それぞれ、RFC2527 をはじめとする一連の RFC などに強く依拠しながらも、独自の CP（CIRTIFICATION　POLICY 認証指針）と、さらに実現可能な詳細な CPS（CERTIFICATION　PLACTICE　STATEMENT　認証

※1 ISOC　INTERNET　SOCIETY　http://www.isoc.org/
※2 IETF　The Internet Engineering Task Force　http://www.ietf.org/
※3 ABA　the American Bar Association　http://www.abanet.org/
※4 RFC2527（Request For Comments 2527）　http://www.ietf.org/rfc/rfc2527.txt

運用規定）を定め、これを公開し、厳正な監査を受けながら、適正な運用を図っている。認証局は、政策と運用規則、失効リストなどの必要文書を公開することで、自ら適正な運用に責任を持つ。これにより利用者、電子署名、認証による証明書を信頼して取引に入るもの（「依存者」、「信頼者」「証明書ユーザー」などと呼ばれる）に対して、まず、透明性を確保し、いつでも誰からでも検討監視が可能なものとすることで、さらには適正な監査制度を採用することで、このシステム、証明書の信頼性を担保しようとするのである。

われわれは、こうした制度提案･運用指針を基礎におきながら、その実用化の実態を検討し、また、わが国における登録制度、証明制度にまつわる法的トラブルの検討を重ね合わせて、合理性を検討しなければならない。

なお、２００２年１月３日、新たなＲＦＣ２５２７のドラフト提案※1 がなされ、６ヶ月間の検討期間に入った。基本的枠組みは変わらないようだが、法的制限の可能性を明記するなど重要な補足説明、内容にわたる議論が始まっているが、変更の可能性を含んでいるので、さらにその動向を注視する必要があると思われる。

0-2 登場人物・機関

電子署名制度には、おおむね次の重要な登場人物がいる。

ＣＡ　認証局（印鑑登録をする登録機関のような存在である）

電子署名を利用しようとする者は、あらかじめ必要書類を添えて登録申請を行い、その審査を得て登録を済ませた後、ＩＣカードなどで内部的に生成された鍵ペアと、認証局によって認証された公開鍵であることを示す証明書とを内蔵したＩＣカードを交付されることになるのが一般のようである。

登録業務を行う機関（ＲＡ）は利用者の便宜で利用者に近いところに設置されることが多く、他方、証明書の発行業務を行う機関（ＣＡ）は安全な集中的管理体制の確保できる専門的な機関が担当するなど、業務分担が行われる場合も多く、そうしたものが一体として一つの責任主体として登場する。

登録者（参加者・利用者・ユーザー※1など）

CA に対して、自ら登録申請を行い、必要書類を提出し、登録によって自らの資格や属性の証明を依頼し、証明書の発行を受ける者である。ＣＡの定めた CP・CPS を承認し、加入契約約款といった契約関係書式を承諾して参加したものである。

※1 ドラフト提案書
http://www.ietf.org/internet-drafts/draft-ietf-pkix-ipki-new-rfc2527-01.txt

※1 RFC2524　2.3　「インターネット PKI のユーザーはクライアント･ソフトウェアを使用する人々およびプロセスです。これらのユーザーは証明書にサブジェクトとして名前が記載されています。」31 頁参照

また、正式な申請をしたが間違えた登録が行われ被害を受けるとか、虚偽の登録をしたのに他人の正式な証明をもらうことで不当な利益を得ることができたといったような、不正行為の加害者、ないし被害者として登場することになる。

依存者（依存者、信頼者、証明書ユーザー※2など）

独特な表現が多いが、CAが発行した証明書を信頼して、取引に入る人、機関、システムなどを広く呼ぶ慣わしのようである。多くの場合CAの発行した、取引相手方に関する証明書を、取引の相手方という立場で受け取り、その証明書の真実性を信頼し、取引を行う立場である。そのため、証明書の真実性にもっとも強い利害関係と関心を持ち、また、多くの場合、トラブルにあって、被害者となる地位である。

電子署名を利用する場合、一方向的に発行され、利用される場合も考えられるが、多くの場合は双方向的に発行され、交換され、相互の認証を基礎におくことが多いと思われる。従って、現実には一つのCAを利用する２当事者間の取引ということも想定されるのであって、こうした場合には多く、一つの契約関係下にはいることがある。こうした場合には、一つのCPSを当事者が承認するため、相互の責任関係は比較的単純になる。その場合はCPSによる一方的免責や損害賠償責任の制限が合理的といえるか、という問題が生じるのみといえる。

ただ、今後多数の CA が成立し、相互に利用可能となるという仕組みを想定するならば、電子署名の交換が双方向的であったとしても、そこで利用される証明書は異なるCAが発行するものであり、相互のCAが相互認証、あるいはブリッジ認証などで結ばれていない場合もある。一方が特定認証局、他方が私的認証局という場合も想定できる。

依存者（信頼者、利用者など）の立場は微妙なため、今後更に検討が必要となると思われる。現時点では、依存者とは、おおむね次のように定義付けられ、考えられている。

RFC2527　2.　DEFINITIONS

Relying party - A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate.　In this document, the terms "certificate user" and "relying party" are used interchangeably.

Relying party（依存する主体） - 証明書を使用して検証された、その証明書、かつ／またはデジタル 署名に依存して振る舞う、その証明書の受け取り手。この文書に おいて「証明書ユーザー」と「relying party（依存する主体）」 という用語は互換的に使われています。

※2 通常の「ユーザー」という定義と、"certificate user"「証明書ユーザー」は区別されている。次頁

日本語訳に関してはすべて、ＩＰＡ　ＩＳＥＣ　情報処理進行事業協会インフォメーションテクノロジー　セキュリティセンター作成の翻訳を引用させていただきました。大変な労作に心から感謝し、利用させていただきましたので、お礼申し上げます。
同ホームページ　http://www.ipa.go.jp/security/rfc/RFC.html

各 CP・CPS においては、認証システムを利用し、証明書の発行を受け、これを利用する関係者に対して、その責任関係・限度を規定し、利用者の承諾の下でこれを運用する建前になっている。さらには、証明書を信頼するものに対しても「依存者同意書」の承諾を義務付けることで責任限定を行っている事例もある※1。

またさらには、RFC2527 の 3.6 では、証明書の中に CPS への参照情報を入れることを含ませるという提案をしている。これによって、CPS を参照できるという仕組みになるが、このことは、必ずしも利用者に責任を負担させるという方向に直結するものではないであろう。また、その参照の仕組みだけで、利用者が CPS のすべてを解読し、それに合意したという擬制（みなす）をするのは疑問である。そのことだけで、責任転嫁とをる合理性もないものと考える。

> **In addition to populating the certificate policies field with the certificate policy identifier, a certification authority may include, in certificates it issues, a reference to its certification practice statement. A standard way to do this, using a certificate policy qualifier, is described in Section 3.4.**
>
> CA は、認証ポリシー フィールドを認証ポリシー識別子とともに埋める ことに加えて、それが発行する証明書の中に、その CPS への参照情報を 含ませることでしょう。これを行うために、認証ポリシー認定子を使用 する基本的なやり方は 3.4 節に記述されています。

RFC2527 で標準化された内容によれば、こうした CP では、何を定め、どのような機能を持つかについて、概括的な定め、ルール化が次のようになされている。

RFC 2527　3.1　CERTIFICATE POLICY

> When a certification authority issues a certificate, it is providing a statement to a certificate user (i.e., a relying party) that a particular public key is bound to a particular entity (the certificate subject). However, the extent to which the certificate user should rely on that statement by the CA needs to be assessed by the certificate user. Different certificates are issued following different practices and procedures, and may be suitable for different applications and/or purposes.

※1 日本認証サービス株式会社　パブリックサービス標準規程　V1.51　2.1.4　依存者の義務

> The X.509 standard defines a certificate policy as "a named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements"[ISO1]. An X.509 Version 3 certificate may contain an indication of certificate policy, which may be used by a certificate user to decide whether or not to trust a certificate for a particular purpose.
>
> 3.1 認証ポリシー
> CA が証明書を発行するとき、証明書ユーザー（つまり、依存する主体）に 特定の公開鍵が特定の主体（認証サブジェクト）に関連付けられている という表明を提供していることになります。しかし、その証明書 ユーザーが CA によるその表明に依存すべき程度については、その 証明書ユーザーによって対応される必要があります。様々な証明書が異なる実践や手続きに従って発行されており、おそらく異なる アプリケーション、かつ／または、目的に適合していることでしょう。
>
> X.509 標準は、認証ポリシーを「 証明書の適用可能性を特定の コミュニティに示し、かつ／または、共通のセキュリティ要件をもった アプリケーションのクラスを示す指定されたルール集 」と定義して います。[ISO1] X.509 v3 証明書は、証明書ユーザーによって特定の 目的のために証明書を信頼してよいか否かを判断するのに使用される 認証ポリシーの表示を含みます。

CP には、一般的にこうした指針を定めるとしているものの、その制限内容は必ずしも画一的ではなく、多くは今後の解釈運用に委ねられているといえる。また、別の観点から、CP・CPS を承諾していない関係者、第三者に関して、何らかの損害が発生した場合には、不法行為責任が発生する可能性も指摘されている（平成１４年３月２９日経済産業省商務情報政策情報経済課「電子商取引準則」※1　成りすまし責任)。

本考察では、こうした法的責任の関係を、電子署名制度の下での認証局の認証業務の実態と、証明内容を基礎にしたうえで、さらには電子署名制度における信頼の基礎としての CRL（Certificate Revocation List　失効リスト）※2 の存在と調査義務の存否、その現実性を考慮して、法的責任を分析するものである。

1　認証システムの体系

責任論の前提として、登録の仕組みと証明の意味について明らかにするのが賢明であろう。ここでは、何を認証するのかに重点を置いて、検討をする。

1.1　個体認証（本人認証）と、登録認証（本人性・法人格認証）

認証（確認の方法）の仕組みとしては、大まかに言って、二つの制度が存在するように思われる。大別すれば、個体認証（本人認証）と、登録認証（本人性・法人格認証）である。前者は固体そのものの特徴によってそのものであることを証明するものであり、

※1 電子商取引準則　平成１４年３月２９日 経済産業省商務情報政策局情報経済課
http://www.meti.go.jp/topic/data/e20329bj.html

※2 CRL の詳細　　http://www.ietf.org/proceedings/01mar/I-D/pkix-new-part1-05.txt

これに対して後者「登録認証」は、事前に特定のものを登録させて、それとその後の申請対象との照合を基本とする証明方法である。

1.1.1 個体（本人）認証

自然人としての存在を証明する制度として、DNA による個体登録と、同一性判断が考えられる。これに類似するものとして、写真による本人確認、網膜や指紋による判断などもこれに類するものと考えられる。これらの制度は、登録された個体と、その後の照合される個体との同一性が自然人の個体としての特徴に依存しているため、自然的存在そのものが証明されることを意図する。この場合、制度によっては形式的登録された氏名などが符合されることがあるが、それは必須ではなく、個体表示が一意に行われれるのであれば符号によっても、あるいは番号などによっても可能である。自然人としての X が、名前ではなく、自然的個体の特徴の符号などによって、自然人 X として認証されるということである。

こうした個体に対する認証, 証明の制度は, 本来的には登録を必須とはしないはずだが、事前登録と組み合わせることでより厳格な運用となるとおもわれる。その人（個体）の表示と確認できればただそれだけで個体の確認ができた，ということになるはずであり、その情報と形式的登録事実との照合を行う制度もある※1。米国でのサインによる確認は、届け出たサインとの一致を問題とするまでもなく，目の前でサインしたこと自体を証明するという形（サイン証明）で発行され，わが国の登記、登録において通用するとされる。身近では、旅行者小切手に対するサインなども，受領者の目の前でサインするということが重要となる。

1.1.2 登録（本人性ないし存在）認証

これに対して、ひとまず自然人の自然的存在から離れて、制度としての登録証明が存在する。一定の制度に登録したということを証明するものである。自然的存在を基礎とすると想定されることが多いが、個体の表示がなされず、登録された事実が確定し、反対に登録された事実が個体を特定し、表示すると言ったシステムである。自然人 X は、自らを A（たとえば戸籍上の名前がそうである）と登録することで、以後、その個体は「A」と表示されることになる。しかし、この登録は、制度上の問題であるため、後に変更することも可能であるし、自ら選んだ名前をもって表示し、認識されることもまれではない※2。

こうした制度登録の証明の典型が法人格の登録である。有機的存在ではなく、個体の存在を前提としない、結節点登録が法人制度である。そこで証明できるのは、個体の存在で

※1 東京商工会議所証明センター

http://www.tokyo-cci.or.jp/shomei/verification_of_registered_signature.htm

※2 氏の変更など　ホームページ裁判所　http://www.courts.go.jp/index.htm#
家事事件　氏の変更　http://courtdomino2.courts.go.jp/T_kaji.nsf

はなく、制度上への登録の事実そのものに過ぎない。

アジア圏の戸籍制度（日本、韓国、中国、台湾などの戸籍関連法ほか）など管理登録制度による証明システムは、むしろ制度として登録されているか、登録された事実のとおりかどうか、ということを問題とするものであって、個体の存在や個体表示とは区別された登録制度に基づく証明、すなわち登録証明になっている。

また，法人の証明に関しても、そもそも法人格というものが実体のない法形式のものである以上、届け出た内容が基礎となり，以後，その届出との差異を検証するという証明方法がとられる。登記簿謄本などを利用した証明・認証方法は，こうした登録を基礎としたもので，証明対象と登録との際の確認が基本となる。

RFC 2527　NOTES

10 Examples of organization identity authentication are: articles of incorporation, duly signed corporate resolutions, company seal, and notarized documents.

11 Examples of individual identity authentication are: biometrics (thumb print, ten finger print, face, palm, and retina scan), driver's license, passport, credit card, company badge, and government badge.

10 組織識別の本人認証の例：設立登記、法的にサインされた会社の決議、 社印、正式なものと証明された文書。

11 個人識別の本人認証の例：バイオメトリクス（親指の指紋、10 本指 の指紋、顔、手のひら、網膜スキャン)、運転免許証、パスポート、 クレジットカード、社員バッジ、政府バッジ。

1.2　区別の利益

これまでこの両者の違いに関してはほとんど考慮されず、その差異を意識した制度作りにも、運用にもなっていなかった。したがって、議論が混乱し、証明の対象も不明確なまま混沌とした議論となってきたものと思われる。

何を証明するのか、が明確にならない限り、なにが証明されているのか、何に対して証明責任が発生するのか、どの点の齟齬に対して責任が発生するのか、など精密な議論の成立は期待できない。両者を明確に区分することで、証明されるもの、責任の範囲が明確になるのであって、その利益は大きいと考えられる。

1.3　具体的検討

わが国における電子署名法に基づく個人認証制度においては、本人確認が行われるが，これらはすべて，まず戸籍制度の存在を前提とし，そこで発行される戸籍を基礎とする。そして，さらには，戸籍を基礎として，あるいは連動した住民登録が行われているので，あわせてそれも基礎とされる。

この他，時として，運転免許証など、顔写真が載っているものの提出を求め、そうしたものの写しが必要書類とされる。

また，これとは別に、「本人限定受け取り郵便」※1による照会書受領書の着信と返信によって、実在することの確認が行われる場合もある（日本認証サービス※2　CPS ３参照)。

以上の実務的取り扱い，多くの場合ＣＰＳによってその内容が例示されているが，内容を具体的に検討すると，異なる意味合いが持たされ，あるいは作用していることがわかる。

戸籍、住民票などによって証明されているのは自然人自体の表示ではなく、届け出られ登録された名義人の登録申請の事実、およびそこから推定された本人の存在だけである。そこで表示された名義人が、どの自然人と一致しているかは関連付けられていない。かりに今後、DNA 登録による戸籍制度ができるか、DNA 登録に一本化されるなど自然科学的に個体の登録が可能な事態に至らない限り、本質的には本人登録・本人証明は不可能である。

現在可能なのは、戸籍などによる本人性（本人登録ではなく、本人として届けられたという事実証明）登録証明と、その後に行われる個体表示（写真などを利用した個体表示）と、本人性登録証明との関連付け（パスポート・運転免許証などの発行制度など）によって、個体証明に近い本人存在証明制度が作られている。しかし、この制度も必ずしも正確な個体表示となるものではなく、その基礎となる戸籍制度上の登録時点での誤登録により、以後の証明はすべて虚偽の証明となる危険性を内包する。

また，これらと平行して利用される「本人限定受取郵便」※1 によって、受取人と表記された者の身分証明書による確認を行った上で交付するこの制度は，本人確認の作業を郵便事業を行う配達局ないししかるべき郵便局によって代行させている。この制度は，電子署名法による本人確認が必要であることから，同法施行後になって急遽作られた制度である。登録する事実と、現実社会での客観的な事実との「紐付け」を行うものであり、制度の客観性を確保するためにはきわめて重要なものである。

ただ，この「本人限定受取郵便」制度も正確には、受取人確認という簡易な仕組みに過ぎず，写真などがなくとも，ただ単に受取人の表示と一致する氏名，ないし関連する名称ないし住所などの提示のみで行われているという。それは，郵便配達の実務運用上最も簡便な受取人確認方法としては致し方のないことであって，それ以上を求めることは事実無理がある。こうして，ごく簡易な受取人確認方法をもって，本人確認に代えているのである。

※1　http://www.post.yusei.go.jp/service/honningentei.shtm　郵便ホームページ
　　http://www.post.yusei.go.jp/service/hongenkakunin.shtm　本人確認資料
※2 日本認証サービス　　http://www.jcsinc.co.jp/
　　CP/CPS　　http://www2.jcsinc.co.jp/repository2/ASignCPS.pdf
※1 本人限定受取郵便　　http://www.post.yusei.go.jp/topic/hongen.shtm
　　100 円の特別料金　http://www.post.yusei.go.jp/ryokin/tokushu.shtm

以上に対して、法人の証明制度※2 はまったく異なる制度となる。そもそも、法人の存在証明の場合には、個体の存在を観念することなく、形式的存在である「法人格」の要件の検討のみで終了する。法的に権利義務が帰属するための結節点であれば良いため、自然的存在の個体との関連性は必ずしも必要ではない。代表権限を持つものの表示も、個体表示と関連させる必要はなく、形式的な申請行為が行われておればよい。たとえば、代表印として届出した印影があれば、誰が申請しても代表印の印影であることの登録がなされ，その印影と同じ印影を持参すれば、同じ印影であるという証明、届け出られた印影と同じであるという証明が発行され、結局代表印であるに違いないと証明されることになる。この証明は、個体の証明や実態の存在をなんら証明しておらず、ただ単に代表印として届けられている印影と同じ印影であることを証明しているに過ぎないし、それで足りるのである。

2　電子認証制度は何を証明するか

2.1　証明の対象

電子証明制度においては、証明対象をどのように特定するか、どのような手続きによって審査するか、それぞれの証明書の性格付けにしたがって、自由に設定できるようになっている。

したがって、個体認証の制度とすることも不可能ではなく、DNA を提出させる方法も今後成立する可能性がある。その場合は、既存の登録制度とは区別される、独自の個体登録が必要となり、制度の安全性確保と個人情報の保護において更に慎重に検討する必要が出てくるのは言うまでもない。

しかし現在行われているものは、すべてが登録証明・登録認証である。

すなわち、個体の存在認証ではなく、法的権利義務の帰属点として、結節点として登録されているであろうことの証明であって、前提となる各種の登録制度の信頼性に依拠するものとなっている。

したがって、個人認証制度のうえで機能する仕組みとされることが多く、法人認証は商業登記制度上の登録法人の制度となることが多い。更には法人の社員、役員といった属性認証に関しては、属性登録制度（社員登録制度）に依存することにもなる。同様に、資格認証、属性認証は、資格登録や属性の登録システムに依拠することになる。こうして、多様な登録制度を背景におくため、証明の度合いもまた多様であり、証明対象、証明の程度、信頼の程度などの多くが、前提となる登録制度の信用性に依存することになる。

弁護士の認証などは、一元管理された弁護士制度登録※1 を基礎とする限り、相当高度な

※2 法人の証明　平成１２年４月１１日に成立、４月１９日に公布された「商業登記法等の一部を改正する法律」の一部（商業登記法の一部改正関係）の施行

※1 弁護士法

認証システムとなるが、コンサルタントという属性、職制の登録に関しては国家による一元管理的な制度はなく、また企業によってもさまざまな位置づけをしており、制度としての信頼性が確定しておらず、この属性認証・属性証明は信頼性が低いということになる。法人役員の証明や、社員証明についても同様である。

2.2　認証局における登録審査(RA局の業務)と責任

審査業務

2.2.1　形式的審査

登録業務を行う登録局（RA：Registration Authority　CA と区別してあえてこう呼ぶことがある）においては、申請者による登録申請を審査することになるが、多くの場合書面審査を中心とする。

ここで審査するのは,「提出された証明書記載事項たる事実」と「登録申請書に記載された事実」との一致の確認である。具体的には個性謄本に記載された氏名と申請者氏名の一致，同様に住民票の住所と申請にかかる住所の一致の確認である[※2]。

中には，写真つき証明書のコピーの郵送を求める私的認証局もあるが，これは明らかに無意味なものである。写真は所持者との照合を行う場合に初めて意味があるのであって、郵送によって書類の形式的審査による場合には,

2.2.2　実質的審査

また，時として，実際の面談による個体の特徴を考慮した、個体存在に関連させる登録（パスポートや運転免許証の提出を求め、かつ、所持人がそこに表示された自然人であることを確認する方法）も用いられることがある。RA 局が、登録希望者の身近にある場合を除いて、現実的なものとはならないと思われる。

2.3　証明の対象（何を証明しているのか）

電子認証による認証局は、証明書によって，何を証明するのか。

2.3.1　存在証明に関するもの

厳密に言えば，登録局に書面として提出された登録済証明書(戸籍謄本など)と、申請名義人との一致のみである。法人の場合で、法人の存在そのものの存在自体を問題とするものや、法人代表者であることを問題とする制度の何れも、商業登記簿に登録された事実と

第八条　弁護士となるには、日本弁護士連合会に備えた弁護士名簿に登録されなければならない。
第九条　弁護士となるには、入会しようとする弁護士会を経て、日本弁護士連合会に登録の請求をしなければならない

※2 日本認証サービス　　CP/CPS　3、同一性の確認と認証

の一致を検討することになる。

こうした証明は，さらに既存の制度（戸籍制度、商業登記制度など）の持つ制度としての信頼性と、その発行する証明書への信頼性、持ち込まれた証明書が通常偽造されていないという社会的慣習に対する信頼性などを総合した、制度全体への信頼を基盤として、提出された証明書類によって証明されている事項は真実登録された事実と考えられるため，間接的に存在事実であるとの推定が働くことになる。

従って，認証局が証明しているのは，極めて単純な事実の一致に過ぎないのだが，前提となる制度の確実性と社会的機能、社会的信頼に基づき、登録事実の存在そのものが強く推定されることになる。

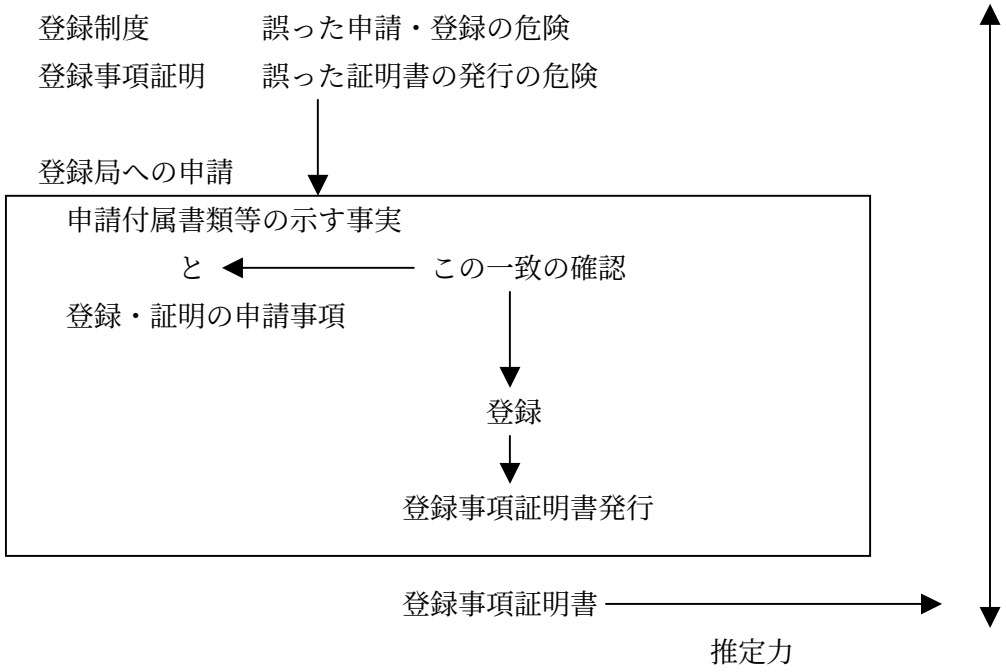
2.3.2　属性証明に関するもの

以上に対して、属性証明にあっては，実に多様であり，その証明内容も，また推定される程度も多様とならざるを得ない。

属性にも，国家試験に基づく資格であるとか，厳格に管理された認定制度であるなどの場合には，戸籍と同様な信頼を与えることも可能となる。こうした場合，証明書は表示された者がその資格を持ち，あるいは認定を受けているという事実自体の存在を証明するものであるし，それを基礎とした登録申請は、そうした証明書の確認に基づいて、申請者との氏名などの同一性に加え，証明申請属性（証明属性）の一致を証明することになるが，その証明の持つ推定は広範囲に，そうした属性の存在，認定資格の存在を推定することになる。

しかし，他方で，属性の中には，登録制度のないものや確認手続きのないもの、たとえば代表者の職務代行者、従業員、代理人といった者であるという事実関係に関しては、それを疎明する一定の書面の提出を求める場合もあるが、そうではなく、単なる申告によってこれを受理する仕組みもあるので、その場合は，申請者の指定があったことの証明となる場合もある。

3　証明の責任



4　証明機関の法的責任　判例検討

4.1　トラブルの実態

これまでの登録証明に関するトラブルがどのように発生してきたか、どのような状況下について検討し、さらにそうした中で、証明機関の責任はどのように検討され、認定されてきたか検討する。

トラブル事例

4.1.1　身分証明書等の目的外使用・不正使用

他人名義の旅券にて不法入国した外国人は、居住する地区の住民としては認められず、住民票、国民健康保険の給付を受けることができない（平成 7 年 9 月 27 日東京地裁判決平６（行ウ）３９号国民健康保険被保険者証不交付処分取消請求事件）とした判例があるが、不正使用した場合、初期の権利（滞在の権利）が保障されないのは当然のことであり、それ以上の言及はなかった。

4.1.2　不正利用に対する表見責任

事案としては、トラブル事案は多数存在する。多くの場合、印鑑証明書、住民票、土地の登記権利書などを第三者が保有しており、それを濫用した場合である。それらの書類を利用して土地等を処分した行為の有効性が問われ、あるいは連帯保証契約を締結された

場合に債務を負うか否かを問う事案が多数存在する。

いずれの場合も、印鑑証明書だけではなく、それ以外の事情を考慮して、信頼者の側の事情を総合して、無過失であるかどうか、個々に慎重に検討して判断している。昭和 50 年 12 月 8 日最高裁第一小法廷判決昭５０（オ）６０８号求償債務不存在確認請求事件、昭和 53 年 5 月 25 日最高裁第一小法廷判決昭５１（オ）５１号土地所有権移転登記抹消登記手続請求事件、昭和 51 年 6 月 25 日最高裁第二小法廷判決昭５０（オ）９７８号約束手形金等請求事件など多数。

4.1.3　偽造した証明書を利用した場合の責任

（あ）　偽造した本人の責任（偽造に協力したものの責任）

偽造罪、及び同行使罪が成立することに争いはない。協力者には幇助犯などが成立する可能性がある。

（い）　偽造されたものの責任

成りすまされた人の責任が問われたケースは見当たらなかった。通常、何らかの与因を提供していると考えられるが、偽造の共犯となる場合はともかくとして、通常の落ち度程度であれば問題とされない。むしろ、被害者であることが多く、責任が問われることはほとんどないものと思われる。

（う）　証明局の証明責任

印鑑証明などの証明を発行する担当部局（多くは市町村の行政機関、通称「役場」の証明係など）が、登録票（事前登録に従って発行された登録カードなど）の提出を受け、あるいは、証明を求める印鑑によって押印した証明申請書を提出させる方法で、それぞれ登録された印鑑である旨の証明書を発行することになる。かねてから印鑑証明書は、登記登録に際して申請者と表示されているものと所有者と同一性の確認に利用されるほか、金銭消費貸借契約の締結などの借り入れ行為の際の契約書に押印した者の本人確認などに多用されてきた歴史がある。印鑑証明書は社会においては本人性の確認と本人の意思確認の一つの重要な補助的方法として広く認められ、信用力の強い証明書となっている。

しかし同時に、印鑑証明書単体では通常なんらの効力も持たず、契約書など本来作成されるべき必要書類などに対する添付書類とされたり、契約において本来は直接意思確認が行われるがその際に確認したという事実の証明のためであったり、付随的に利用されるのが通例である。

こうした関係から、法的論点としては次の点が浮かび上がってくる。

A　登録や証明の際の照合作業においてどの程度の注意義務が必要か
通常人の通常の注意義務か、特殊な注意義務が必要か
肉眼による比較検討で足りるか、機械的照合の必要があるか

B　証明行為と信頼行為との因果関係
印鑑証明などを、事実と間違えて登録し、あるいは証明をした場合や、真正な証明書を本来交付、発行してはならない場合に誤発行し、本来発行してはならない人に間違えて発行した場合などに、その印鑑証明を利用され、具体的に発生した被害、またその発生した損害との因果関係はあるのか
故意に申請書を偽造した者や、詐欺行為によって真正な印鑑証明を発行させた者の介在などの事情の存在は因果関係を遮断するか

C　損害額に対する証明書の関与の度合い
被害を受けたもの（証明書を信頼して出損し、被害を受けた者）が、信頼したことが正当か否か、信頼することに重大な過失はないか、いくつかの過失が重なったり競合したりしていないか

これらの各論点を検討するために、これまでの登録証明機関の落ち度（過失）による損害賠償請求事件を概観して、わが国における登録証明をめぐる法的権利関係を考察したい。

4.2　判例の検討

ここでは、これまで議論されてきた著名な判決から、特に印鑑証明制度を中心とした登録証明制度において、何らかの登録ミス、あるいは故意によって発生した証明書の誤発行に基づく損害の発生を基礎にして、その被害の賠償責任をどのように判断し、拡大、因果関係をそのように制限したか、さらには発生した損害の配分（過失相殺）のあり方について、検討を加えるものである。

4.2.1　①印影比較の過失（否定　見た目で判断して疑義ければ責任なし）

平成 13 年 2 月 6 日東京地裁判決平１１（ワ）２０４８０号損害賠償請求事件

事案

印鑑証明書の発行を担当する登記官は、本来登録された印影と、証明を求められた印影とが照合できるかを審査して、証明をなすべき義務があるところ、印鑑照合の際その差異に気づかず、偽造された印鑑による印影を登録された原告の印影である旨の印鑑証明書を発行したため、その印鑑証明書を使用されて原告が所有する土

地、建物に無断で所有権移転登記などがされた事案である。土地所有者が、移転した土地は取り戻せたものの、取り戻しにかかった費用などを求めて、国に対し、損害賠償を求めたのである。

判旨

裁判所は、届出印の陰影と証明を求められた印影の両者の間には、客観的に大きな差異が数点あることは認めたものの、「印鑑証明書の趣旨及びその重要性からすれば、印鑑証明書を発行する登記官は、申請書に押捺された印影と登録されている印影との同一性について、登記官として社会通念上一般に期待される業務上相当の注意をもって照合すべき注意義務があるというべきであるが、具体的には、両印影を近接させて肉眼で両印影の大きさ、形状、字体等に差異がないかどうかを子細に照合すればよく、その照合によりわずかでも疑いがあるときには、拡大鏡や印鑑対照検査機を用いるなど、より精密な方法を用いて照合する義務があるというべきである。」としつつも、求められる判断方法とは、「登記官の過失の有無を判断するにあたり本件印影と登録印影との差異を比較検討するに際しても、拡大された印影を比較検討するのではなく、実際に本件印鑑証明書（申請書）に顕出された本件印影と印鑑登録原簿に顕出された登録印影とをその実物大に即して比較検討すべきであるということができる。」とし、本事例では、まず、「本件印影と登録印影とは、その大きさ、形状、字体及び文字の配列が極めて類似しており、肉眼で子細に照合してもその差異を識別することが極めて困難であり」なおかつ、比較的差が明確であると認められる相違点についても、「その部分に差異のあることを前提にするのではなく、このような前提のない段階において比較検討した場合には、両印影を近接させて肉眼で子細に照合しても、その差異を識別することは極めて困難である。」として、過失を否定したのである。

評釈

この判決は、登記官が、登録された陰影と証明を求められた印影の両者を近接させ、肉眼で、通常の注意義務で比較検討し、類似しているかどうか、明らかな差がないかどうか、疑わしき点はないかを注意すれば足りるのであって、それ以上の注意義務を求めていない。

この点では、このほか昭和４１年１０月２１日最高裁第二小法廷判決、昭和５０年５月２７日最高裁判所第三小法廷判決などがある。昭和５０年の最高裁の判断でも「同一性に疑義がない時まで常に拡大鏡を使用し、または両印影を重ね合わせるとか剣先を用いてその真偽を確認する義務はない」と判断している。

一般に不動産取引の場合、登記全般を委任される司法書士は、受領した正式に発行された印鑑証明書と、契約書などに押印された印影とを重ねあわせたうえで、一方を何度となくめくり、また合わせ、を繰り返すことで両印影の子細な照合を行う

ことが見られる。それに比較して、両印影を近接させて比較するというのはいささか安易にわたるように思われるが、大量に処理する登記官の負担を考慮すれば、この程度の注意義務を求めるのが現実的というべきであろうか。

認証局における印鑑証明書の印影と申請書類の印影との照合は、登記官に類似する程度の注意義務を求められることになると思われる。

4.2.2 ②なりすまし・印影比較責任（責任否定 ①類似）

平成13年3月5日東京地裁判決平１２（ワ）５８４７号損害賠償請求事件

事案

偽造された印鑑証明書を利用して、他人の自動車登録が抹消され、これを知らずに自動車を購入した者が、後に真実の所有者から返還請求を求められ、売却せざるを得なかった事案で、購入価格と売却価格との差額が損害であるとして、国に対し、損害賠償を請求した。

判旨

自動車の登録変更[※1]の申請があった場合、「その審査に際しては、陸運支局長は、申請者の意思確認の真否を判定するための有力な手段として、印鑑証明書（同１６条１項）に押捺された印影と代理権限を証する書面たる委任状（同１４条１項３号）に押捺された印影とを照合すべきこととなるが、同照合義務の具体的方法及び程度は、前記の陸運支局長（自動車登録官）の審査権の性質を考慮すれば、肉眼で対照して各印影の大きさ、型、字体、文字数等に差違がないかどうかを検討し、各書面の形式的真正の有無を判定し、明白に不真正な書類に基づくものであるとの疑いが存する場合は、これを不受理、不登録とすべき注意義務を負うけれども、陸運支局長（自動車登録官）の注意義務は、同程度にとどまるものと解するのが相当である。」として、印鑑証明書の審査については、「一般的にみて、権限のある発行機関によって作成されたと認められる外観を有しているか否かは審査すべきであるが、その外観上明白に不真正な印鑑証明書であるとの疑いが生じる等特段の事情がない限り、それ以上に、当該印鑑証明書が、真に法令等に則り、適式な手段で作成されたものであるかどうかまで調査する義務は存在しないと解すべきである。」として、外観上明白な疑いのない以上、これを承認したことに過失はないと判断した。

評釈

この判決も、発行された印鑑証明書と、委任状の比較検討を行うべき立場にあるが、この場合でも特段の疑いがもたれるようなものでない限り、通常の注意義務により肉眼で比較検討すれば足りるとしたものである。

従って、認証局での受理審査とほぼ同じ作業を行うことになるので、注意義務のレ

※1 自動車登録の手続き　財団法人自動車検査登録協力会　　http://www.aira.or.jp/entry/entry.html

ベルにおいてもほぼ同レベルのものが求められ、それで足りるように思われる。

4.2.3　③成りすまし見逃し責任(否定　身分証明書などの外観を基礎に判断)

平成 8 年 12 月 19 日福岡高裁判決平７（ネ）９５６号不正印鑑登録証明書交付国家賠償請求事件

事案

偽造の無線従事者免許証を持参して、偽装にかかる印鑑登録廃止届等を提出した者からこれを受理し、右免許証に基づいて本人と判断・誤信して、これに基づいて印鑑登録廃止・印鑑登録・印鑑登録証明書の交付をしたため、この印鑑証明書などを信じて土地売買を行い、土地代金８０００万円を詐取されたとして、市職員の過失を問題とした事案。

判旨

まず、印鑑登録を担当する職員が、その廃止届けを受理するに当たり、本人であることの確認を行う義務があるが、「本件のごとき本人の同一性確認について、印鑑登録・証明事務の担当職員に国家賠償法一条一項にいう過失があったというためには、平均的な印鑑登録・証明事務の担当者であれば右の同一性につき当然に疑念をいだいたであろうと考えられるのに、事務担当者の職務行為に合理性が欠けていたために、疑念をいだかないまま事務処理を遂行したと認められることを要すると解するのが相当である。」とした上で、身分証明書の偽造に関しても、これを見破ることは困難であったと判断した。すなわち「無線従事者免許証の体裁をとっており、九州電波監理局長なる印影が顕出され、貼付された写真と台紙にかけて割印があり、記載事項自体は真正な無線従事者免許証と同一であって、全体がラミネート加工されていたから、平均的な事務担当者がこれを偽造免許証であると見破ることは困難であったといわざるをえない。」とし、さらに付随事情として「本件免許証に記載された昭和六年八月一四日生まれの男性という点でほぼ一致していたうえ、態度も通常の申請人と特に変わった点はなく、落ち着いた様子であったというのであるから、甲野と乙山本人との同一性について疑念をいだかせるような事情はなかったというべきである。」という認定を行い、「本件免許証の提示によって、甲野を乙山本人と誤信したことはやむをえなかったものといわざるをえない。そして、田畑及び柴原は、甲野が乙山本人であることを前提に、通常どおり、条例、規則、要領及び事務処理慣行に従って事務処理を行ったものであって、その過程においても、特段、甲野が乙山本人ではないのではないかとの疑念をいだくような事情があったとは認められない。」と判断して、職員の過失はなかったとの結論に至っている。

評釈

この判決では、偽造された身分証明書の概観上の特徴によって、特段疑わしき点がなかったという点に加えて、さらに、年齢の判断、申請時の挙動など、総合的に判断

するという姿勢をとっており、総合的判断によって過失がなかったとしたものである。
本人の同一性判断の判断基準、事情を示すものとして興味深い。

4.2.4　④無権限による証明書発行の責任

(重過失肯定　因果関係肯定、過失相殺適用）

平成１年３月１５日福岡高裁判決（上告）判例時報１３２４号４９頁

事案

市議の依頼により、印鑑登録証明申請書もなく、本人の意思確認もしないまま印鑑証明を発行したが、その印鑑証明書を利用して、高利貸しから３回にわたって借り入れを起こしたが、その借り入れが焦げ付いたため、高利貸しが原告となって市に焦げ付いた１億８０００万円の損害賠償を求めた事案

判旨

たとえ顔見知りの市議の依頼があったとしても、印鑑登録書もなく、本人の意思確認もなく印鑑証明書を発行したのは明らかに過失がある。なお、当該市議にも過失があり、共同不法行為となる。

しかし、３回にわたる借り入れ行為のうち、後の２回については保証人が必要となり、保証人の印鑑証明書が必須となったことからすれば、仮に印鑑証明書がなければ融資が実現していなかったといえるので、２回目、３回目の融資合計額１億３９６５万円に関しては因果関係があるといえる。

ところが、貸し金業者としては、「本件貸付けをするにあたり、本人Ａ及び保証人Ｂの職業、資産状態、信用等のほかＡの借入金の使途、返済計画等の調査をすべき義務あるところ、これを怠った重大な過失があったものといわなければならない。

もし、一審原告において、直接Ｂの保証意思を確認する労を厭わなければ、Ａの虚言は直ちに発覚し、本件貸付はこれを容易に避け得たところである。」として、金融業者としての本来求められる注意を全く果たしていなかった事実、むしろ、本来調査すべき当然の事実関係や保証意思の確認すら行っていない事実に鑑みて、貸し金業者の過失が９割であると判断、印鑑証明の誤発行の過失割合は１割だと判断、結局損害の１割に当たる１３９６万円の損害賠償を、市に対して認めた。

評釈

印鑑証明書が間違えて発行されたことにより、契約が締結された事実から見れば、因果関係の広がりとしては、印鑑証明書を利用した契約の多くが認められることになるのはやむをえないといえる。

しかし、印鑑証明書の発行費用が極めて小額のものであること、印鑑証明書の発行が極めて正確に行われているかといえば必ずしもそうでない場合も多く、従って、発行に係る負担とその影響力の開きをどう解すべきか、困難なところである。

幸い、本件では印鑑証明書の利用があったとしても、ほかに本来履践すべき基礎

作業があるにもかかわらず、それを懈怠した重大な過失があったので、結論として発行局は打撃的な損害の大部分を回避することができた。しかし、特段の事情などがあり、過失相殺が簡単に行えない場合には多額の損害を負担することにもなる。

公的存在であり低廉な仕組みでなければならないこと、危険に比較して収入は小さくバランスが取れていないこと、危険分散の発想が必要ではないか、など疑問なしとしない。電気通信事業者の回線事故などの場合の損害賠償額制限の仕組みと比較して、さらに議論すべき問題を含んでいると考える。

4.2.5　⑤成りすまし証明発行の責任(本人意思の欠如を認め慰謝料として責任肯定)

平成５年７月１９日名古屋地裁判決（一部控訴）判例時報１５０５号１２０頁

事案

遺産分割協議に基づく登記などに利用するため、本人の意思に基づかないで共同相続人が印鑑証明を申請することになり、意を知った印鑑証明手続きを担当していた上司に相談して、本人申請の書類を作成し、印鑑証明を発行した事案。ただし、遺産分割協議自体は本人参加の下で行われていたため、意思に反して印鑑証明書が発行されたという点で、慰謝料の賠償請求となった。

判旨

まず、印鑑登録をするには、本人に右申請の事実を照会し、回答書を持参させる等して登録申請が本人の意思に基づくものであることを確認するべきであった（条例第四条一項、二項）にもかかわらず、これをせず、何らの記載もない回答書にX（職員）自ら本人名を記載して同回答書を作成し、本人の印鑑登録を行い、さらに虚偽の印鑑登録証明交付申請書に基づき印鑑登録証明書を作成し、交付したことが認められるとして、この市の職員は条例第四条一項、二項等に違反するもので、少なくとも重大な過失があると判断した。

ただ、損害額に関しては、使用目的が本来の合意に沿うものであったことから、具体的な実害・損害は認定されず、意に反したという点での慰謝料１０万円が認められたに過ぎない。

4.2.6　⑥成りすまし見逃し責任（過失責任肯定　因果関係あり　過失相殺）

平成１年３月２９日大阪高裁判決（確定）　判例時報１３２４号４９頁

昭和６３年三月２４日神戸地裁尼崎支部判決判例時報１３００号９９頁

事案

他人とその共謀者が、本人の印鑑証明書を取得するため、本人に代わり、本人のすでに存在する登録済みの印鑑につき、紛失申請を行い、それに変わる新しい印鑑の登録申請を行うとともに、印鑑証明の発行を依頼して事案で、共謀者が、本人と同地域の居住することから保証人となり、共謀の上、本人の意思を保証する旨の虚偽の保証

を行ったため、市当局はこれを安易に信頼して、新規登録された印鑑証明書を発行したが、それが利用されて、金銭消費貸借に利用され、４５００万円が詐取されたという事案

判旨

判決はまず、全体の考え方に関して、次のような指摘をする。

「最近における印鑑証明書の使用目的の拡大及び発行数の増加のため、第一審被告伊丹市その他の地方自治体における印鑑登録事務及び印鑑証明書発行事務が多忙となり、地方自治体に相当大きな負担をかけていることは、これを窺うに難くない。

しかし、反面において、印鑑証明書制度は国民生活に深く定着し不動産をはじめとする重要な財産の保全や処分に至大の関係を有する制度であり、国民が地方自治体の印鑑証明書発行事務の正確性に高度の信頼をおいて財産取引を行っているのも事実であって、地方自治体の事務の繁忙のゆえにたやすくその事務取扱いが簡略化・形骸化され担当職員の注意義務が軽減されてよいものではない。」　と指摘して、注意義務が安易に軽減されない旨判断した。

本件では、同地域に居住する保証人により本人であるとの保証がなされたという事情があるため、市の職員が安易に印鑑証明書を発行したのであるが、こうした簡略化された方式があるからといって「当該規定に形式的に準拠したからといって必ず国家賠償法上の過失がないことになるものではないと解される。」という厳しい判断をした。

そして、過失の有無に関しては、次のように判断した。

「従前の印鑑の廃止届、新印鑑（偽造印鑑）の登録、新印鑑の印鑑証明書の交付申請の三者が一時に申し出られたのであって、通常一般的に生ずる事例ではなかったのであるから、とくに慎重に本人の意思が確かめられるべきは当然であり、同市内に印鑑登録をしている共謀者により申出人が本人である旨の保証がなされた（いわゆる保証人方式）とはいえ、保証人方式は照会書郵送方式や写真付公的証明書方式に比し本人（の意思）確認の手段としてかなり劣っているのであるから、担当職員は、条例一六条により、申出者に質問権を行使したり適宜の資料（名刺のごときものでも同じものを二枚以上所持しておればかなりの資料となる。）を呈示させたりして、その者が本人であるかどうか更に確認することこそ右条例・規則の趣旨に適合するゆえんであるといわねばならない。」と判断して、こうした注意を払わないことに関して、過失を認めた。

なお、一審も同様に、登録時しか本人意思の確認はできないケースであって、登録時に慎重に対応することが必要であるとし、条例１６条に定める質問調査権を適切に行使して、必要事項を口頭で言わせ、さらに本人しか知らない家族構成、本籍などを言わせ、あるいは疎明資料（写真付の書類など）を提出させるなど等差を尽くすべきであるとして、過失を認定している。

犯人らが、この印鑑証明書を利用して、本人の持っている土地を担保に借り入れを

起こして、４５００万円の焦げ付きを作った事実を認めたものの、貸し付けたほうの重大な過失を認定、１審は８割の、控訴審で９割の過失を貸し付けた側に認めたため、市の過失部分は損害額の１割である４５０万円になると判断した。貸し金業者は、貸し付けるに当たり、自宅を訪問するとか、電話にて本人意思を確認するなどしておらず、また本人確認の方法も、生命保険料の支払い領収書程度で済ませており、むしろこうした書類では本人確認をしていない現状からすれば、かえって疑うべきであり、慎重な確認をしていないことが重大な過失であるとした。

評釈

この判例は、前記④の判例とほぼ同様な判断をしており、参考となる。むしろ、証明者に対して、的確な質問調査権があるということを基礎に、慎重に判断すべきであるとしている点で、むしろ注意義務としては高い認定をしていると解する余地もあるが、そのように理解すべきではない。

右判決は、いずれも、間接方式の中でも、とくに保証方式の脆弱性を繰り返し指摘しており、むしろ立法政策上の問題と考えられるべき性格のものである。これが直ちに証明局の注意義務一般の問題となるとも考えられず、他の判例と同様な程度の注意義務を認めているものと考える。同種事案に平成４年２月１９日大阪地方裁判所判決、平成６年５月２５日奈良地裁判決などがある。いずれも国家賠償法に基づく公共団体の責任を認め、また、同様に大幅な過失相殺（９割）を認める判断をしている（奈良地裁)。

4.3　判例実務のまとめ

以上の参考判例を概観してみた場合、おおむね判例の立場として次のようにまとめることができる。

Ａ　登録や証明の際の照合作業においてどの程度の注意義務が必要か

この点に関しては、証明書を発行する立場であっても、特殊な注意義務が必要というわけではなく、通常人の通常の注意義務を果たすことで足りるとする。通常注意すればわかるはずであるのに、漫然と注意をすることもなく見過ごしたといった場合に過失を認めており、むしろ重過失に近いほどの任務懈怠が指摘されている場合が多い。特に照合に関しては、司法書士が行うような、慎重に重ね合わせる検証作業や、拡大鏡を利用した比較検討や、機械的照合の必要があるかについては、全くその必要性を認めていない、というのが実際である。

Ｂ　証明行為と信頼行為との因果関係

印鑑証明のケースでは、過失のあるケースでは因果関係が認められており、信頼性の高い証明書である分、明確な因果関係が肯定されるようである。第三者が介在し、証明書を

利用したといったケースがほとんどであるが、他人の故意が介在しても、あるいは故意に虚偽の印鑑証明書の交付請求がなされて利用されたとしても、因果関係が否定されることはないといえる。この点は、刑事事件の因果関係とは大きく異なり、損害の発生との関連性というプラスマイナスにおいては相当強い関係が肯定されることになる。

C　損害額に対する証明者の過失の割合（過失相殺　　民法第４１８条、７２２条）

被害に対する寄与の程度においては、証明機関の寄与はおおむね１割程度の小さなものになるようである。こうした証明書は、ただそれだけでは信用されず、添付書類として利用されることが多く、他の事情による総合的判断が求められることになる。取引における対価性の確保の必要は当然にあり、担保を取るとか、保証をつけるとか、直接会って確認するなどの作業が求められる。多くの場合、本来確認すべき点を確認せず、なぜか、孤立した証明書だけに頼るといった異常さがあり、通常の取引者が守るべき注意義務の範囲を大幅に逸脱していることにより、そこに被害者の大きな過失を認定し、証明局の過失との間でバランスをとっているのである。常識的な注意をしなかった取引者に９割の過失があるとし、証明局には１割の過失があるとして、全体の被害の１割だけを証明局に負担させるという判断となる。

また、注意すべきは、印鑑証明の発行手続きが後に述べるような電電公社などと類似した公的サービスの提供という点では、広くあまねく提供されるべきであることから、あまりにコストのかかる義務の負荷や過大な注意義務を負担させることには消極的という姿勢を持つ点である。

しかし同時に、印鑑証明書の果たす役割、特に不動産取引などにおいてしめる重要性に鑑みると、その信頼性ゆえに大きな責任があるという事実は否定できないとも言う（判決⑥他）。従って、証明書の果たす役割、証明書に対する社会的信頼度を考慮して、判断する必要性が指摘されている。

この点、前者の公的サービスによる責任限定を認めた制度、そしてこの制度を正面から認めた判例として、次の事案が重要である。

4.4 ⑦世田谷地下ケーブル火災事件（インフラ障害裁判　責任限定　）

東京地方裁判所判決平成１年４月１３日判例時報１３１９号７８頁

通信ケーブル火災損害賠償請求訴訟

事案

昭和５９年１１月旧日本電電公社・現ＮＴＴ世田谷電話局管内世田谷通り地下通信ケーブル専用構内で，工事中に火災が発生しケーブルが燃えた為，加入電話回線は切断などされて，最長で１０日間不通となった事件で，近隣の回線利用者である商店主らが売上減少の営業損害など４７００万円を請求した（世田谷通信ケーブル火災損害

賠償請求訴訟)。

判旨

東京地裁は，火災原因が，工事施行会社の下請けに属する２名の作業員の過失であることを認定したものの，電電公社は工事の実施にあたって十分な注意と指導を行っており，事故防止義務を尽くしていると認定し，管理者たる地位にある電電公社には、作業員の過失による事故発生の危険性の予見可能性はなく，管理上の注意義務違反、すなわち過失もないと判断した。従って，法的構成の如何にかかわることなく，過失がなく、責任を追う理由がないため、被害を受けた原告らには損害賠償請求権がないとして，請求を棄却したものである。なお、控訴審である東京高裁は，前提として，電電公社は公衆電気通信法１０９条（その後電気通信事業法に改正）の損害賠償額限定規定を優先的に適用され，国家賠償法などの請求はできないと判断した。すなわち、電電公社が公的性格をもち、広く国民に対して低廉な通信料による通信サービスの提供を実現する為には，損害賠償額を通信回線使用料の５倍までに制限することの妥当性があると判断した。しかし、本件訴訟においては、原告らが電話使用料の５倍の金額を請求しているとは考えられない為，１部分の認容もできず，控訴を棄却するとの判断となったのである。

その後，公社が廃止され，現ＮＴＴに改組し，現在はＮＴＴサービス約款[※1]に従って処理されることになったが，それによれば、過去６ヶ月間の使用料の平均額を基礎にして，日割り計算した分を損害とする，ということになる。

4.5　リアルトラブルとオンライントラブルの違い

以上、印鑑証明制度におけるトラブルにおける判例の示す法的責任論を概観した。

その特徴は、印鑑証明という重要性にかんがみて、発生した損害に対する責任の可能性を肯定した上で、過失相殺で救済した、といってよい。

ところが、オンライントラブルの場合、その目指すスキームにおける証明書の重要性は印鑑証明と変わるところはない。むしろ、オンラインでの唯一の身分証明という点では印鑑証明よりもより重要な役割を持つとも考えられる。従って、責任の重さという意味では特段の違いはないかもしれない。

しかし、広がり（因果関係）と過失相殺については大きな違いが生じる可能性がある。まず、因果関係に関しては電子的な関連性という意味では記録も残り、立証も簡易であり、その広がりは正確に把握できる。その有る無しは明確であるといえる。相当因果関係という広がりの制限が必要なケースもあるかもしれないが今後の検討のなかで個別具体的に究明されるものとなるだろう。次に、過失相殺はどうか。相手（信頼者、依存者、証明書ユーザーなど）の過失とはいったい何か、である。オンラインで考えられる相手の過失は比

※1 ＮＴＴ電話サービス約款　８７条
http://www.ntt-west.co.jp/tariff/yakkan/denwa/denwa-07.html#12a

較的単純である。言ってしまえば電子署名の信頼性の確認に尽きるだろう。それ以外の多くのリアルな因子が使えるのであればそれはそれで認証局の責任減殺の方向で動くことになるだろうし、信頼者の特別事情として考慮されることがあるかもしれない。しかし、原則的には証明書の信頼性、契約の信頼性はオンラインという平板な世界で確認されることになる。オンラインの特段のシステム（同時履行確保のための相互供託確保サービス「エスクローサービス」※1 など）を採用するという手段もあるが、迅速で、簡便さとスピードが優先されるオンライン取引が常にエスクローサービスを選択するとも言い切れない。

では、証明書の発行をめぐるいくつかのミス、信頼の基礎の脆弱性に基づく損害の発生の責任はどのように配分すべきであろうか。電子署名が社会を流通する信頼であるとすれば、現在の印鑑証明と同様、大きな責任を担う必要があるだろう。そこでの責任分担は、やはり合理的な責任配分でなければならないだろう。民間事業者が提供するサービスである以上、必要以上のコスト負担は企業経営を不能にするだろうし、しかしだからといって、認証局を強く免責することは無責任な制度を作ることにもなり、妥当とは思われない。したがって、責任分担、配分は、証明局に置いて、証明局の負担で、信頼者の過度の負担なく、簡便に確認できる方法（サービス）を提供し、にもかかわらず信頼者に期待することが合理的で、かつ簡易に履行できる注意義務を果たさなかった場合にはその取引に起因する責任の過半を負担してもらう等の合理的な仕組みを基礎にすべきであろう。そうであるとすれば、証明書の信頼性を裏付けると考えられる、現在の最良の手段である CRL（失効リスト）の簡便な確認方法、OCSP（Online Certificate Status Protocol　自動失効リスト確認システム）※1 の提供こそが責任転換の合理的基礎と思われるのである。信頼者には、こうした簡便に、自動的に証明書の信頼性、有効性を確認できる手段を提供されるべきであるし、もし仮にこうした確認システムを提供されていながらあえてそれを使わない、というのであれば、そのリスクは自ら負担するのも当然と考えるであろう。

こう考えると、認証局は、証明書の発行と失効管理を的確に行うべき立場にあり、これを故意、過失によって怠ったため、信頼者、依存者、利用者らによる受領証明書の確認のための CRL の確認、OCSP の確認に対して正確に回答できなかった、という場合にはそこから発生した被害の全額を補償すべきことになる。これは、認証局のミスとして責任を負うべき部分であり、その額の多寡にかかわらずこの結論が妥当であろう。この額が大きくなるからといって、責任転嫁を図るのは妥当ではないだろう。認証局の企業としての経営安定は、保険システムの採用などを考慮して総合的に対処すべきものといえる。

※1 YAHOO オークションエスクローサービス http://event.yahoo.co.jp/docs/event/escrow/guide05.html
ヤマト運輸　宅配便エスクロサービス　http://escrow.kuronekoyamato.co.jp/

※1 OCSP　OCSP に関する RFC は下記に明記されている。 Request for Comments: 2560
X.509 Internet Public Key Infrastructure Online Certificate Status Protocol - OCSP

現在進行中の RFC2527 の再検討において、責任制限の方法として、個別当事者に対する責任限定と、事故全体における総合的な責任限定をかのうにするほうがいいだろうといった視点で提案がなされているようであるが、こうした責任限定は安易にしてはならず、契約内の限定的合意事項として機能するにとどめるべきものであると解する。

保険制度による信頼性の確保のほか、今ひとつの可能性として、多様な属性認証サービスの提供、あるいは多様な証明サービスの相互補完の形態が形成される可能性があると思われる。銀行口座の存在確認サービス、あるいは支払い保証サービス、ソフトウエアやサービスに関しては著作権登録証明サービスや資格認証サービス、オンラインでの事業者供託金サービスなどの提供も考えられる。

さらには、複数の証明書を提出することで保険が安くなるとか、料金を一定限度割り引くなど、責任分散原理と複合的な証明書の保管作用によって、飛躍的に信頼性が高まるという性格を利用することが考えられる。

こうして、オンラインサービスを補充するきわめて多様なサービスが発展することで、こうした責任の更なる合理的分担が可能になると思われる。ただ、現在こうしたサービスがほとんど存在せず、あるいは一般に提供されていない段階で、あえて信頼性があると断言するには、一定の保険のバックアップを得て、事業者である認証局が責任を負担して、信頼の制度を支える覚悟を持つ必要があるだろう[※2]。

こうした観点からみれば、オンラインでの証明書の信頼性の確認はオンラインで簡便に行えるように求めるべきであり、責任転換（信頼者に責任を負担させること）は慎重でなければならない。

CP/CPS で、責任転換を規定すればそれで責任転換を承諾したことになるとの発想は合理的根拠を欠くものと言われかねない。そうした転換が合理的であるという仕組み、責任転換をしても信頼者を大きく害することはない、過度の負担を負わせることにはならない、という仕組みの提供が必要である。

さて、公的サービスという点を見た場合、電子認証局は、電子認証制度を支えるインフラ的存在であり、証明書を発行する機能としては、印鑑証明書を発行する機関と基本的に変わるところはない。証明書を発行するというサービスが、広くあまねく実施され、低廉で、誰もが利用できるようになるのが理想であり、多くの認証局は公的性格を認識し、証明書発行業務を遂行している。その点では、典型的なインフラをささえていた旧電電公社に対してその運用の保護を図る目的をもった損害賠償額の制限（賠償額を通信回線使用料の５倍までに制限すること）は相当強い合理性を持つものといってよい。

※2 後記マイクロソフト偽証明書事件での、ベリサイン社の責任転嫁しようとは思っていない」とデ・シルバが述べたが、その姿勢は評価すべきものがある。後記 28 頁参照

しかし、この事案は、通信インフラの提供ではあっても、提供された側は便利さを提供されただけであって、信頼の基礎を提供されたわけではない。電電公社が、何らかの証明行為を行っていたわけでもない。従って、回線途絶による障害という流通阻害という損失以外は発生することはなかった。

ところが認証局が発行する証明書は、電子商取引において極めて重要な証明書であり、信頼の基礎を提供しているものであって、信頼という側面では印鑑証明書と同様な位置付けになると思われる。

さらに困難な問題は、印鑑証明書はリアルワールドにおいて、多面的な検証装置、仕組みの中で比較して小さな割合を持つに過ぎないとされるが、これに対して電子商取引における電子書名とその認証によって発行される電子証明書は、オンラインという限定された世界においてのみ機能するものであることから、印鑑証明と比較して、全体における割合が大きくなる可能性がある、という点である。

印鑑証明書にあっては、証明書が単体で機能する場面はほとんどなく、むしろ他の主要な書類、契約書などの付属書類としての役割を持つという点で、リアルな関係における多面的検証方法が提供されている分、その果たす役割が比較して小さくなっているといえる。ところが、電子書名の認証、それによって発行される証明書にあっては、オンラインでの判断においては、いわば唯一の資料とされる可能性がある。リアルな社会での面談や、口頭での質問、挙動の確認、本人意思の確認方法の多様性といったものがすべて捨象され、本人確認の方法としての電子署名の交付が求められ、それで足りると考えられる事が多い。ただ、現実には、過去の取引事例がない場合に極端に高額な取引をはじめるなどといった事例はオンラインにおいても軽率のそしりを免れないし、オンライン決済にあっても前記のような「エスクローサービス」（相互供託サービス）を利用することはいわば常識となってきているので、証明書だけで信頼され、実行されるということは少ないように思われる。オンラインでの存在証明としての電子署名にあっては危険性は少ないといえるが、今後さらに充実するであろう属性認証、属性の証明を含んだ電子署名にあっては、属性の持つ強い信用力、属性自体の重要性に鑑みると、より大きな比重を持つ可能性も否定できない。

さらには、印鑑証明書は転々流通する危険性はないし、特定当事者間の一回のみの特定取引に利用されるだけで、それで利用は終了し、それ以上に利用されることは通常予想されない（登記の際、原本還付[※1]といった方法によって印鑑証明書を還付する方法もあるが通常３ヶ月しか証明力がないとされており、転々流通する可能性はほとんどない）。ところが、電子署名にあっては取引者が無数、不特定多数という場合が予想され、こうした場合の証明書の発行の被害は世界中にひろがる危険性を持つ。

[※1] 印鑑証明書の原本還付　昭和 40 年７月７日地方法務局からの照会に対する民事局長回答
http://www.soumu.go.jp/kansatu/fudo.htm
http://www.koshoku.or.jp/qanda/prev.asp?page=63

すでに発生した事故報告で、その危険性を強く認識することができる。

マイクロソフトの発表によれば、マイクロソフトの従業員をよそおった人物が２００１年1月30日から31日にかけて、デジタル署名を発行している米ベリサイン （カリフォルニア州マウンテンビュー） をだまして、2 種類の証明書をマイクロソフトの名前で発行させるという事件が発生し、この事実が同年３月２２日に公表されたという事件である。当時の新聞記事によると、この事件は、マイクロソフト従業員と名乗る成りすまし犯の証明書発行申請に応じて、申請者への照会をすることなく、その成りすまし犯に対してマイクロソフト社の正規の製品であるとの証明書を発行してしまったというのである。その後、マイクロソフト社は、この証明書を向こうとするパッチを発行したが、全世界６０億台のPCにインストゥールされる可能性は低く、問題は解決していない。

> 「通常、ベリサインは、適切な要求を受けてから新しい証明書を与えている。ベリサインのアプライドサービス部門副社長兼統括責任者のマヒ・デ・シルバは、同社がどのように要求の真偽を確かめるかについて詳しくは語らなかったが、「人為的なミスによって、身分を偽った人物がマイクロソフトで働いていた時期が判別できなかった。実際はマイクロソフトで働いてはいなかった」と述べた。
>
> 新たな証明書の発行要求を受けたあと、ベリサインは、その新しいコードを注文した顧客に電子メールで確認する。今回の場合、「(マイクロソフトから)返答が得られるまでにしばらく時間がかかった」とデシルバは語った。ベリサインはマイクロソフトから返答があって初めて、その証明書を発行するべきではなかったことに気づいた。
>
> 「間違って証明書を発行してしまったが、第 2 段階の不正防止機能によって、今回の間違いが発見できた。責任転嫁しようとは思っていない」とデ・シルバは述べた。
>
> ベリサインが誤ってコードを発行したのは、今回の 2 つの証明書が初めてだ、とデ・シルバは述べ、これまでに50万件以上の証明書を発行していることに言及した。『Class 3』証明書は、顧客――今回の場合はマイクロソフト――に対して、最高10万ドルの損害賠償を保証している。
>
> CNET Japan Tech News「マイクロソフト、偽のデジタル証明書を警告」 By Robert Lemos/日本語版 喜多智栄子 Thu 22 Mar 2001 14:40 PT

こうした場合、ソフトウエアのダウンロードを行うに際して、信頼すべきものはそのソフトウエアを配布する者の信頼性であり、その証明が電子署名に他ならない。そして、ソフトウエアの購入と、ダウンロードにあっては、電子署名以外の方法による検証の余地は与えられていない。唯一安全な方法は、購入しない、ダウンロードしないという手段だけとなる。こうしたソフトウエアのオンライン取引などの場合における電子証明書の重要性は明らかである。ここでの過失による偽証明書の及ぼす被害は世界中に広がる危険性があり、その額は相当高額なものとなるとも考えられる。

事故発生後、マイクロソフトによる偽の証明書のものを摘示するソフトウエア、パッチ

といわれるソフトが提供されていたため、慎重な利用者はこれをインストールして、対策を施しているとも考えられるが、すべての利用者に同様な対処を求めることはできない。従って、こうした事故の発生、被害の拡大を防止するには、偽の証明書がオンラインですぐに検証され、自動的にCRL（失効リスト）を検証するサービスが提供されなければならない。OCSPレスポンダの普及が解決の糸口と思われる。

マイクロソフトケースにおいても、ソフトウエアをダウンロードする際に、証明書が出るが、その検証を自動的にできるようにして、その際ワンクリックでOCSPが稼動して、即座に回答するという仕組みであれば、そして無効証明が見事に出されるとなれば、安全性を確保することができる。そうした裏づけがあって初めて、オンラインの証明書は信頼に足るものとなるはずである。

4.6　事故の想定

認証局の注意義務と責任

認証局の注意義務の内容

認証局、特に登録局ＲＡにおいては、申請書の審査を行うことが必要であり、正確な登録が行われる必要がある。また、CA 局（証明書発行局）においては、正確な記録に基づいて、正確に発行することが必要となる。

① 登録ミス　正確に申請したのに間違えた登録となっている
- 名前や、商号の誤記入など
- 有効期限や登録日などの誤記入

② 成りすまし登録

本来してはならない架空名登録
- 架空人の登録（架空人への成りすまし）
- 他人の名前などによる登録（他人への成りすまし）
- 法人でないものの法人登録など（法人成りすまし）

③ 発行ミス
- 取り違え発行（受取人の取り違え）
- 証明書、鍵の取り違え（他人の鍵を交付など）
- 非登録者への発行

不可避的な、あるいは人的攻撃による事故を除外した場合、通常問題の発生は単純な人的ミスによって起きることが予想される。

証明書発行における人的ミスは、すでに発生しており、参考例として貴重な研究対象となっている。

５　信頼の基礎　　CRL

5.1　CRL の法的性格

オンラインでの証明書への信頼は、オンラインでの証明書検証手続きと一体となる以外にこれを客観的に、制度的に支えることはできないし、こうした検証手続きなくして、証明書のみを信頼の対象とすることは、制度としても脆弱というほかない。

この点 RFC は慎重に対応している。すなわち、総論的な仕組みとして、証明書の失効リストの設置とこれの照会を利用者・依存者に義務付けるというものである。

RFC2527　4.2.1 Obligations
* Relying party obligations:

    * Purposes for which certificate is used;
    * Digital signature verification responsibilities;
    * Revocation and suspension checking responsibilities; and
    * Acknowledgment of applicable liability caps and warranties.

* 依存する主体の義務
* 証明書が使用される目的
* デジタル署名検証の義務
* 失効と留保をチェックする義務
* 適用可能な依存可能性の限度と権利の承諾

さらに、CRL に関する詳細を定めた Request for Comments: 2459、インターネット X.509 公開鍵インフラストラクチャ （ Internet X.509 Public Key Infrastructure Certificate and CRL Profile ） の指針によって、CRL の重要性を示して、次のように規定している。

2.3 User Expectations

Users of the Internet PKI are people and processes who use client software and are the subjects named in certificates. These uses include readers and writers of electronic mail, the clients for WWW browsers, WWW servers, and the key manager for IPsec within a router.

This profile recognizes the limitations of the platforms these users employ and the limitations in sophistication and attentiveness of the users themselves. This manifests itself in minimal user configuration responsibility (e.g., trusted CA keys, rules), explicit platform usage constraints within the certificate, certification path constraints which shield the user from many malicious actions, and applications which sensibly automate validation functions.

2.3 ユーザーの想定

インターネット PKI のユーザーはクライアント・ソフトウェアを使用する人々およびプロセスです。これらのユーザーは証明書にサブジェクトとして名前が記載されています。これらのユーザーとは、電子メールを出す人や受取る人、WWW ブラウザーのクライアント、WWW サーバー、およびルーター内の IPsec キー・マネージャーなどです。本仕様書の方針は、これらのユーザーが使用するプラットフォームの限界、およびユーザー自身の能力と注意深さの限界を認識したものとなっています。このため、本方針は、ユーザーの最低限の設定責任(たとえば信用のおける CA キー、規則など)、証明書内におけるプラットフォーム使用上の明確な制約、ユーザーを悪意の諸行為から保護する証明書パスの制約、および確認機能を敏感に自動化するアプリケーションを明示しています。

こうして、証明書が多くの利用者に利用されること、彼らが必ずしも強い注意力を持っているとは限らないこと、従って、RFC は、通常の契約参加者、CPS を承諾した利用者としてのユーザーの最低限の責任や、確認作業の自動化の必要性（OCSP レスポンダーなどの仕組み、アプリケーションを意味すると考えられる）を指摘するものとなっている。

これに加え、単なる信頼者、依存者、証明書ユーザーに関しては、更なる詳細なケアーが必須となると考えるのである。

5.2 失効リスト作成義務

証明書が何らかの理由で失効した場合、それを的確に管理することが安全性確保の前提である。そのため RFC は、失効の原因を明確にして、ＣＡは確実に失効リストを作成すべき旨を定める。

3.3 Revocation

When a certificate is issued, it is expected to be in use for its entire validity period. However, various circumstances may cause a certificate to become invalid prior to the expiration of the validity period. Such circumstances include change of name, change of association between subject and CA (e.g., an employee terminates employment with an organization), and compromise or suspected compromise of the corresponding private key. Under such circumstances, the CA needs to revoke the certificate.

3.3 取消し

証明書は、発行されると有効期限内は使用できるのが普通です。しかし状況

によっては有効期限が切れる前に証明書が無効になることもあります。このような状況としては、名称の変更、サブジェクトと CA との関係の変更 (たとえば従業員が退職するなど)、および対応する秘密鍵が改ざんされたか改ざんされた可能性がある場合などがあります。このような状況では、CA はその証明書を取消す必要があります。

こうした規定に従って、各 CA は、失効リストの作成に関し、詳細な規定を持つに至っている。ただ、同時に RFC は、必ずしもこれを義務付けているわけでもないが、こうした制度自体の完備を求めていることは明らかである。すなわち、

5 CRL and CRL Extensions Profile

Conforming CAs are not required to issue CRLs if other revocation or certificate status mechanisms are provided.

5 CRL と CRL エクステンションの方針

適合 CA は、他の取消し機構あるいは証明書ステータス機構が設けられていれば、CRL を必ずしも発行する必要はありません。

として、他の代替手段が存在している場合に限って、CRL を省略することを認めるのであるが、オンラインでの処理が簡便であり、確実であるため、ほぼすべての CA は、CRL を設置し、これを公開し、検証の基礎を提供している。

5.3 失効リストの確認

CRL を公開し、それを調べるように求めること、義務付けることは可能であるとしても、果たしてその作業が、すべての利用者に要求できるのか、という問題がある。

そこで、簡単に、自動的に処理できる仕組みとして、OCSP が考案され提供されている。

すなわち RFC２５６０によって、提供されている仕組みが利用者に自動的な検証を可能とするアプリケーションである。

RFC2560

2. Protocol Overview

In lieu of or as a supplement to checking against a periodic CRL, it may be necessary to obtain timely information regarding the revocation status of a certificate (cf. [RFC2459], Section 3.3).

Examples include high-value funds transfer or large stock trades.

2．プロトコル概要 English

周期発行 CRL(periodic CRL)による確認方法の補助やその代わりとして、証明書の失効状態 ([RFC2459]の 3.3 章参照)に関する情報を適時(タイムリー)に取得することが必要な場合があります。例として、高額な送金あるいは大口の証券取引などが挙げられます。

これが、現在進行中の OCSP であるが、すべての CA が実装しているという段階にはいたっていない。

ところが、OCSP では完全でないとして、さらに現在検討されているのは、次のような仕組みである。

――――――――――――――――――――――――――――――

4.3.4 今後の拡張

OCSP を用いると、CRL による有効性検証の処理を証明書利用者が行わなくてよいというメリットがあります。しかし、OCSP は証明書が失効されているかどうかを確認するだけであり、証明書の有効性を検証するための証明書のパス構築と検証は、証明書利用者が実施しなければなりません。これらの処理は証明書利用者にとって、負荷のかかるものとなります。そこで、サーバ側で失効状態の確認だけでなく、証明書のパス構築と検証までを行う方式が IETF によって検討されています。

現在(2002 年 3 月)では、以下の 2 種類のドラフトが提出されています。

(1) DPD + DPV

OCSP を拡張し、証明書パス構築(DPD: Delegated Path Discovery)と証明書パス検証(DPV: Delegated Path Validation)を連携させる。

(2) SCVP

シンプル証明書検証プロトコル(SCVP: Simple Certificate Validation Protocol)を使用する。

IETF では、同じような標準を 2 つ定めないことになっているので、この 2 種類のどちらかの方式が採用されると考えられます。

---

http://www.ipa.go.jp/security/pki/043.html

情報処理振興事業協会セキュリティセンター　isec-info@ipa.go.jp

PKI 関連技術解説　より引用

5.4　日本認証サービスの採用している仕組み

CP・CPS によれば、

「2･1･4

依存者は、リポジトリにて公開される「依存者同意書」に同意しなければならない。そこに明記されているように、依存者は、取引相手である加入者の証明書の有効性についてチェックしなければならない。」　として、証明書の有効性を自ら検証する義務を課している。

また、セコムトラストネット　セコムパスポート for Web　サービス CPS　によれば、次の

様に規定する。

――――――――――――――――――――――――――――――――

4.4.10 CRL のチェックに関する要件
信頼当事者は、自分が信頼しようとする Entrust.net SSL Web Server 証明書が失効していないかをチェックしなければなりません。自分が信頼しようとする Entrust.net SSL WebServer 証明書が失効していないかを確認するために、信頼当事者は、適切なリポジトリに記録されている証明書失効リスト（CRL）をチェックします。Entrust.net、Entrust.net SSLWeb Server CA が認定する独立の第三者 RA、再販者または販売協業者、もしくはその下請業者、卸売業者、代理店、供給業者、従業員、または役員は、(1)信頼当事者が Entrust.netSSL Web Server 証明書の失効または期限切れの確認を怠ったこと、あるいは(2)失効済みまたは期限切れの Entrust.net SSL Web Server 証明書を信頼当事者が信頼したことが原因で発生したいかなる損害についても、責任を負うものではありません。

――――――――――――――――――――――――――――――――

さらに、日本認証サービスの場合は、責任限定の合理性に関して、依存者に対するの責任限定を「依存者に対しては依存者同意書で定める金額を上限とする。」と明記し、損害賠償責任の範囲を限定した。

5.5 オープン PKI とクローズド PKI

CALS の採用する PKI は、国土交通省が管理するクローズド PKI ということができるであろう。CRL などが作成されるが、会員には非公開であり、国土交通省など入札を受けるものにしか明らかにされない仕組みを採用しているようである。

また、現在検討されている地方自治体の個人認証制度もまた、公的機関にしか開かれないクローズド PKI となる見込みである。

こうしたクローズドな PKI においては、証明書の利用者は公的機関、指定企業以外ありえないし、そうした証明書の信頼者は国家、地方公共団体、特定認証局などの専門機関であり、CRL の確認は日常業務として当然行うものであって、こうした機関に関して特段の考慮はいらない。内部的に CRL が開示されておれば良いだろう。

しかし、これに対して、信頼者が広く一般利用者に拡大されているオープン PKI においては、信頼の基礎を明確にする必要があるだろう。この場合は、不法行為的な側面を考慮することになる。

以上に対して、セミクローズドな PKI も存在する。CP/CPS を承諾したものしか利用できないクローズドマーケット内での利用者は、すべて当該 CP/CPS によって拘束されることになるので、契約関係を有するものということができる。従って、当事者における特別な契約による拘束、すなわち責任限定も、非合理でない限り、有効と見ることができる。

6 まとめ

この論考を通して、電子署名制度によって証明できるのが、登録事項であること、そしてクローズドＰＫＩであれば契約約款ないし、その基礎となるＣＰ／ＣＰＳを承諾することで一定の契約責任、責任制限が可能であることを指摘した。同時に、その対極にあるオープンＰＫＩにあっては、信頼者の責任を無条件に認め、ＣＲＬを確認しないときには何

がおきてもＣＡは免責される、とする現行の仕組みは、信頼性にかけ、問題がある旨指摘した。

もともと、ＣＡができるのは、存在証明ではなく、登録事項証明であるとすれば、その信頼構造、責任内容もまた、信頼性のある制度とするには、慣習が支えている信頼の制度というべき印鑑証明制度的なものとして構想され、達成されなければならない。そこで、判例を概観して責任制度を見たが、過失相殺という巧みな手法で責任制限をしたが、オンラインではまだそうした過失相殺の事情は発達しておらず、現時点では拡大の可能性も孕む。しかし、同時にオンライン証明制度には、必然的にその証明書の確認という作業が付随しているという新しい常識を普及させることが必要であって、そのためには簡単で、確実な確認検証方法を提供して、その利用を促進し、それに対する信頼を確保することが必要と考えた。それがＯＣＳＰであるが、現在こうした仕組みを採用しているところは少ない。しかし、ＩＳＯＣでの議論はさらに進んで、その先を見ている。

ＣＡの法的責任を回避することが、ＣＡを中心とする電子署名制度を発展させることにはならないのではないか。むしろ，ＣＡに対して厳しい内容となるも、利用者、信頼者にとって合理的制度であること、提供された便利さを、あえて利用しないことで危険性を覚悟している場合には、その契約に関する責任を負担させるという思考は合理的なのではないか。その便利な仕組みは、ＣＲＬではなく、ＯＣＳＰであると考える。新しいニュースでは、オープンソース系で、自由に利用できるＯＣＳＰが提供される予定であるという。定かではないが、そうした動きは必然であろう。

わが国には、大変有意義なマーク制度がある。このマーク制度も存在することのみではなく、さらにそのマークが簡易に検証できることが必須の条件であり、利用者がそのマークに触ればそれだけで、偽造でないマークとして認証され、確認されるという制度が採用されつつある。

証明書も、簡単に利用できなければ普及はしない。それに、解読困難なCP･CPSの中で巧妙に免責をかけて逃げたのでは、利用者は全く救われないだろう。それでは信頼の制度は確立しない。信頼の制度を確立するには、保険制度を背景に持ちながら、事業者が一定のリスクを負う必要がある。その上で、そのリスクを最小限にする努力は、利用者への責任転嫁や挙証責任転換といった観点からではなく、全体としてセキュアーな契約、権利関係を確保するスキームを考えることである。

ＣＡの作業をする人々、事業者に対し、心から尊敬の念を持ちつつ、更なる勇気を持って、新しい信頼の礎を作る作業に邁進されることを期待するものである。そのために法律ができること、しなければならないことは山ほどある。われわれ法律実務家は問題を技術者に任せきりにすることなく，必要なことを確実に進める必要がある。

法的部門からは、迅速な問題解決を推進すべくＡＤＲ（Alternative Dispute Resolution

代替的紛争解決)の設置を進める義務があるだろう※1。また、こうした分野の専門家を育成する必要性も高い。なお、道は険しいが、不退転の決意で、歩を進める決意である。

ＲＦＣ　の翻訳は全面的にＩＰＡ情報処理振興事業協会　ＩＰＡセキュリティセンターの参照資料として提供された翻訳※2に従った。心から感謝するものである。

牧野二郎

２００２年４月１０日脱稿

※1 ＡＤＲの紹介　ADR-JAPAN　http://www.adr.gr.jp/
※2 IPA セキュリティセンター　ＲＦＣ資料 http://www.ipa.go.jp/security/rfc/RFC.html