電子認証をめぐる法律関係

認証関連事故をめぐる関係者の過失と責任に関する考察

2002年5月27日　　弁護士　牧野二郎

ⓓ- 0, May 27, 2002, Version 1.0 Jiro MAKINO

概要

本論文は、電子署名制度を信頼できる制度とするためには、認証局が自らの責任を回避することなく引き受けること、そのためには利用者の「正当な信頼」を保護する仕組みが必要であると主張する。従来社会の証明書は検証の仕組みに富んでいるが、検証をオンラインで処理しようとする電子署名の場合には、現実社会よりもさらに高度で、利用しやすい検証の仕組み、安全の仕組みが必要である。オンラインのリスクの多くは、利用者に負担させず、認証局が自ら負担すべきである。

認証事故による損害の拡大については、利用者に負担させるという立場をとらず、認証局がすべての責任を取ることで、制度の信頼性・利用者の利便性の向上を確保する選択を試みた。

さらに、登録者には認証局との契約上の責任と証明書取得者（契約当事者）との契約上の責任の二面性、登録局には契約上の責任とインフラ確保の社会的、公的責任をそれぞれ肯定すべきとし、反対に証明書取得者（信頼者）に対しては法的義務・責任は負担させず、検証による信頼を保護されるべき地位を認めるという構成を採用した。こうして証明書利用者の信頼を確保し、利便性を高め、活用できるインフラとしての位置づけを行うものである。

キーワード

認証局の責任　責任の限定　依存規約　依存者同意書　失効登録
失効登録のタイムラグ　認証局の公的地位　正当な信頼　依存者の責任

関連性（リンクは最終ページ）

基礎とした議論：特になし

参考としたもの

電子署名利用者システムの構築・利用ガイドライン

批判検討対象：　各認証局のCP,CPS

電子商取引等に関する準則

産業構造審議会情報経済分科会ルール整備小委員会

認証局の責任に関する提言　ECOM/認証公証WG

関連論文：　電子認証局の法的責任

目次

1. はじめに

電子署名と認証システムが稼動を始め、いよいよ現実的な問題となってきた。平成 13 年度のＢ－Ｂの分野での「ｅマーケット・プレイス」の市場規模は４兆円に達し、さらに順調に進展しているという報告※1がなされ、さらにその成長率は毎年前年度比 150%を超えるものとなっているといわれ、いよいよ「ｅマーケット・プレイス」※2という存在が実態のある確かなものに成長してきたということができる。

ところが、電子署名制度はこうした電子商取引を牽引するべく登場したにもかかわらず、その牽引役を果たしているとは言いがたい。いまだにＩＤ、パスワードのほうが便利、といわれ続け、その本来のメリットが活かされないでいるのが実情である。

※1 経済産業省・ＥＣＯＭ・ＮＴＴデータ経営研究所の共同調査結果「平成 13 年度電子商取引に関する市場規模・実態調査」概要

http://www.meti.go.jp/kohosys/press/0002379/
http://www.meti.go.jp/kohosys/press/0002379/0/020218ec.pdf

※2 その範囲については、「『売り手、買い手ともに複数の事業者が参加するオープンな電子商取引の共通プラットフォーム』に限定している。」として、明確な定義が与えられ、独立した数字がカウントされた。ただ、これらがすべて電子署名を利用している訳ではない。

電子署名は、本来のオープンなオンライン社会での認証システムとして機能するものとして構築されたはずであるが、残念なことに現時点での主な利用方法は「アクセスコントロール」であって、クローズドＰＫＩとも言うべき限定的な役割しか実現できていない。クローズドなマーケットでは、そもそも同一基盤上の同一の管理局によるコントロールであることから組織内の他の統制力（コミュニティの同質性による慣習、組織内ルール、規約など）が働くため、特別な装置は必要ではない。その意味で、安全のための「アクセスコントロール」という観点であればＩＤパスワードでも十分である。それでもあえてクローズドなマーケットで電子署名制度を採用するメリットといえば、電子署名にすればパスワードの変更といった面倒で、混乱の原因となる作業を回避できるという点など、そう多くはない。

本来予定すべきオープンなネットワークでの電子商取引は、未知のものとの取引であるため、相当しっかりした基盤が用意されない限り、信頼を確保することはできない。オープンマーケットだからこそ、成りすまし、偽造、自己否認という問題が生じるのであり、その対策が重要になるのである。こうした観点から、電子署名制度が提案されたのであって、ＩＤパスワード代わりという目的ではなかったことを認識しなければならない。

かつてインターネットの普及のさなか、ビル・ゲイツ氏などによりイントラネットが主張され、その後両者は車の両輪のごとく急速に発展・普及してきた。クローズドＰＫＩとオープンＰＫＩは、あたかもこの両者のように車の両輪のように発展していくのであろうか。

Eマーケット・プレイスをはじめとする電子商取引の発展に伴って、それを悪用する事例、システムの脆弱性に起因する事故の発生など、多様な問題が発生することは避けられない。電子署名制度が人類初の試みであることから、コンセンサスを得ることが困難であり、研究、啓蒙、そして情報を共有する努力を怠っていては本物の制度とならないことはいうまでもない。

ここでは、電子署名、その認証証明をめぐる関係当事者の法的関係を検討し、事故が発生した場合の責任分岐を検討するものである。従って、認証局を巡る、登録者、利用者、契約者、名義を利用されたものなど、多数の当事者の法的関係を検討することになる。

電子認証に関する法的分析は、既に「認証局の責任に関する提言」（ECOM/認証公証WG）※3によって詳細に検討されている。しかし、認証局の経営基盤を重視し

※ 3 平成12年3月公表　http://www.ecom.or.jp/report/wg2-2/e11-cn3.pdf

て責任配分を行う意図が基礎にあるため、国民、事業者に広く利用される信頼の制度として提言されているとは思われない。事業者である認証局は、取るべき責任を取るという明確な立場をとらない限り、誰も信用しないと考えるので、本論文では、認証局の取るべき責任を正面から肯定する立論となっている。

1.1. 認証にかかわる事故の発生

1.1.1. 電子認証の流れ

電子署名に対する証明書を認証局が発行し、その後、その証明書が契約当事者、相手方に交付送信され、それが信頼されて、電子署名と認証局の証明書が資料となり、オンラインで契約が締結される。それに基づき、直ちにソフトウエアが提供され、あるいはサービスが提供され、決済されることがある。また、貸借や、売買代金の決済は、オンライン銀行を通して、あるいは既存の銀行に対する現実の資金の移動の指示としてなされるなどする。あるいはさらに現実社会とリンクして、動産、不動産などの所有権の移動・登記や利用権・担保権などの設定行為・登録行為が行われるなどもする。こうして電子署名・認証を基盤とした信頼関係を基礎に、その電子証明書を利用した取引が広範に行われる（図 1 参照）。

同様なことは、リアルな世界では、従来から極めて慎重に多重にチェックされてきている。当事者の身分や事業がチェックされ、銀行が介在することで、信用が審査され、手形などが利用されることで資金の存在が示される。不動産業者が物件を調査し、聴き取りをし、役所に確認するなど事前調査を行う。司法書士が土地の存在、権利の帰属の真実性を調査し移転を確実にする。弁護士が契約書を作成するなどして、契約全般に法的注意を払う。また、現実に契約に立会い、取引の安全性や履行方法、取引条件などのチェックを行う。公証人は債務の履行を確保するために公正証書を作成するなどの行為を行う。こうした幾重にも重なる検査の継続の中で現実の取引が実現するように制度化され、ルールとなっている。

このリアルな現実社旗での取引の局面と比較して、オンラインでの契約や証明書関連のチェックシステムは、いまだ成長中であって、完全なものとはなっていないようである。現実社会以上の信頼性を確保する仕組みとするには、さらに慎重な枠組み、責任分担、保険など各種の仕組みの構築が必要である。

通常の利用方法と流れ図

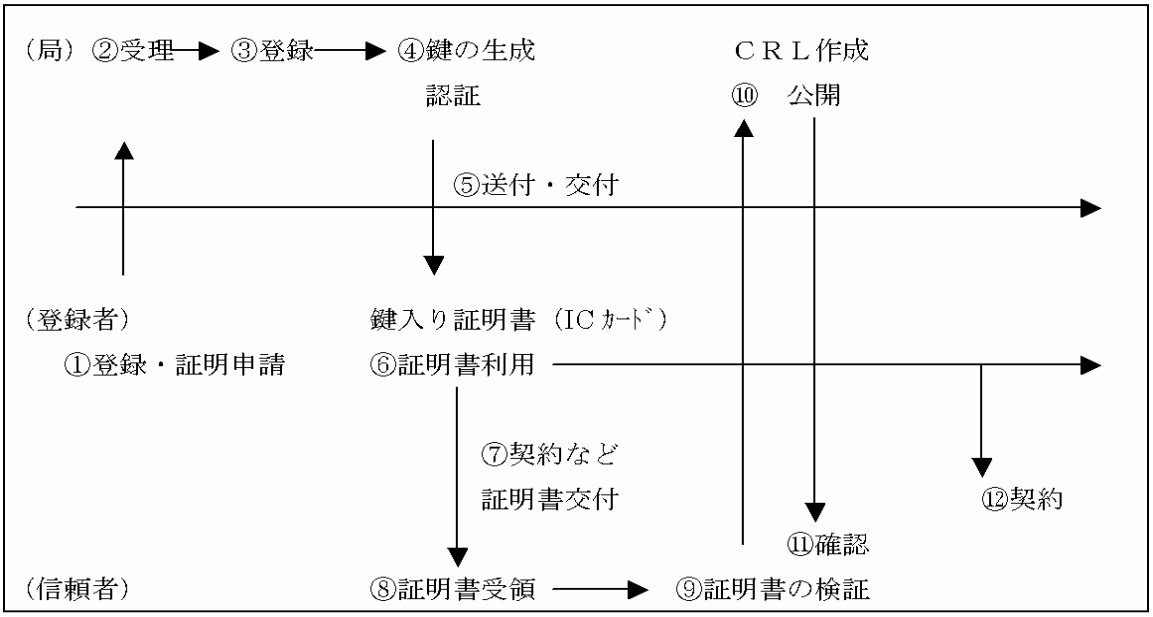

図１

通常①から順次⑪まで進み、取引が完了する。さらに別の契約⑫が始まるが、当初利用したものと同じ⑤の証明書が利用される。

1.1.2. 事故の発生とチェックの機能低下

ただ、リアルな社会がこうした慎重な仕組みによって支えられているはずなのに、皮肉なことに現実は必ずしも期待通りには進まない。相当慎重なチェックシステムを事実上備えているはずのリアルワールドでの取引に関しても、他人の印鑑証明書や委任状を無断で持ち歩く人間がいる。他人に成りすまして他人の住民票をとり、それを悪用することもまだまだ簡単にできるようである。こうして、慎重な仕組みを持っているはずの現実社会も、存外脆弱な面を併せ持つのである。

一方電子的世界、すなわちオンラインでの取引において、果たして期待されるほどの現実と同様な、慎重で幾重にも重なるようなチェックシステムが構築されているか、といえばそうではない。現在のところ、唯一といっていいチェックシステムが、電子署名・認証とその検証の仕組みである。オンラインでは、その仕組みが、データの流通に限定されているため、諸関係が立体的構造を構成するようにはなっておらず、１本の回線を通した情報がすべてのように考えられがちである。すべてをその情報のみに頼ろうとする。そこから、信頼の構造がどうしても平板になりやすく、その結果、リアルな社会にあるような重層的で、複雑で、

多様に入り組んだ安全な「信頼の仕組み」を作り上げることが、比較的困難となる。その中で、電子署名制度が困難な船出をし、現在ようやくその第一歩が記された形である。

ここで注意しなければならないのは、仕組みを考える立場では、既存の信頼システムに基礎を置き、しっかりとした錨（いかり）を下ろしたものとして構成するという点である。少なくとも平板なるゆえに、順次虚構が成立し、虚構の永久循環に陥るような危険は可能な限り排斥しなければならない。他方、利用者の立場では、オンラインで簡単に利用できるようにしながら、かつ、他のデジタルデータ相互で保証を補完しあい、検証ができ、保証されていることがわかる仕組みを作らなければならない。利用者にリアルワールドとの接触を求めるような現実的な検証を要求したのでは、電子署名制度はその存在意義を失ってしまうだろう。利用者に対しては、オンラインのみで、そして簡単に検証できて、信頼が保護される仕組みを提供しなければならない。

こうした観点から、今後、さらに幾重にも重なるチェックシステムが構築されなければならないし、それは、現実社会の脆弱性をも克服するものであってほしい。電子署名制度だけを孤立させ、批判に任せるようなことをしてはならないし、大いに工夫して、新しい支援の仕組みを構築する必要がある。

1.1.3. 実践的な試み

たとえば、オンラインのシステムのうち、幾つかの重要なポイントごとにリアルワールドとリンクさせ、あるいはオンラインの仕組みを現実の制度の上に定着させるべく、しっかりと錨（いかり）を下ろさせる必要がある。シンガポールでは、契約の成立はお互いの信頼が基礎になると考えて、可能な限り現実的な社会での契約行為を重視する。その上で、様々な手続きはすべてオンラインで行うといったすみわけが意識的に進められているが、これもまた、現実の既存の信頼に基礎を置く、錨を下ろすという意味で重要な知恵なのである。

また、電子的に発行させる証明書に関しても、別の認証局が発行する別の証明書の提出を求め、そうした証明書を提出したものを優待するなどして、複数の根拠を示させることで数段の確実性を確保することができる。複数の証明書を要求すること、あるいは他の種類の情報、出来れば異なる根拠によって生成された情報など相互の証明書や情報の比較検討、情報の相互チェックを行うといった手法は重要である。電子的情報の重なり合いを重視することで、情報の持つ確実性は飛躍的に向上するのだから、こうした工夫も積極的に採用されるべきである。

電子署名制度自体は、意思表示の属人性を保証するという有用な仕組みであるが、その立脚基盤をわが国では印鑑証明などの現行制度の上に置いた。従って、機能は高度であっても、オンラインの上でのチェックシステムは、これまでの印鑑証明書の発行ないし公正証書作成の意味の程度を超えることのない、むしろ至って平板なチェックシステムとして構築されている以上、その仕組みにリアルワールド以上の完全を求めることは困難かもしれない。リアルなシステム（住民票や印鑑証明で存在確認を行う制度）を基礎にして作られ、運用されている電子署名制度に対して、基礎となる仕組み以上の完全性、無謬性を求めるのは酷な話であるともいえる。

しかし、データという特性を考慮するとき、むしろ、オンラインの仕組みはデータの単一性ゆえに大きな危険を内包するのであるから、それを前提にさらに強力な様々な工夫がなされなければならないのではないか。加えて、システムや、利用方法が定式化・標準化されていないため、利用者はさまざま環境におかれ、異なる作業を求められる結果、予想外の事故の発生の危険性にさらされているといった状況にもある。

こうした証明書の発行、あるいは発行された証明書の利用にかかわる事故発生に伴う、被害補填の法的責任配分はきわめて微妙な問題を包含する。しかし、こうした事故に対して、誰も責任を取らない仕組みを構築したのでは「角を矯めて牛を殺す」ことになり、本末転倒の結果となる。利用者にとって、あるいは信頼者にとって、リーズナブルな仕組みであることが、普及のために必須であることも事実である。

1.1.4. 法的検討の対象

電子署名制度の法的解釈や証明書の推定力に関する議論に加え、現実の運用を見据えた法的責任を明確にし、関係者の法的責任を議論する必要性は高い。

問題とすべき電子署名の関係者としては、①登録申請を行う電子署名利用者、②その申請を受け付け、証明を行う認証局、③その認証局の発行した証明書、認証の行われた電子署名付文書を信用し、これを利用する証明書利用者（信頼者）、さらには④成りすましの場合には､｢成りすまされた本人｣が関与することになる。

法的関係の議論の基礎には、当事者の法的関係が存在する。まず、①電子署名利用者は、②の認証局との間で電子認証サービス契約といった内容の契約関係にあり、両者の間は、ＣＰ、ＣＰＳ、ならびに契約約款で整理されることになる。さらに証明書取得者である③は、通常は①の電子署名利用者との間で、何らかの契約（売買契約、プログラム利用契約、サービス提供契約などのさまざまな契約）が締結され、その際、当事者の存在証明ないし属性証明として認証された電子証明書を交付することになるが、契約の中で、電子署名が有効であることを保障す

るなどの内容が盛り込まれ、あるいは契約の債務の１要素として正確な証明書の交付が求められることになる。不動産売買契約の際の印鑑証明書、住民票の交付いったものに類似した（正確には不動産売買の際の必須書類であるという点でより強く求められているため、意味合いは異なる）ものとなるだろう。

ところが興味深いのは、認証局②と、証明書取得者（信頼者）③の関係である。両者の間には直接の契約関係はない。ところが、ＣＰＳの中には、「依存者同意書」の類のものがありこれを同意して利用するものという記載を持つものがある※４。

証明書利用者は、本体となる契約締結などの際に、証明書を当然に受け取るのであって、証明書を発行した特定の認証局のＣＰＳなどを確認して、その認証局にアクセスして、認証局との間で何らかの合意を確立させ、その証明書に対する利用許諾を行うとは思えない。多くの場合、利用するブラウザがあらかじめ認めたルート認証局を基盤とする証明書を、利用者の意思とは無関係に自動的に受容し、あるいは所定の証明書を自動的に受容するよう設定され、自動的に単純に検証のみを行って、確認されればそれで終了するはずである。その際、正確には契約締結以前に、交付予定の当該証明書の認証局との間に何らかの合意があるかといえば、ないというほかない。

仮に、日本認証サービスのCPSがいうような「依存者同意書」が存在しても、その存在を確認することもない。証明書利用者（信頼者）が、一定の合意をしてから利用するといった擬制はきわめて不自然である。むしろ、証明書取得者は一般的に信頼されている認証局のものであれば、特段拒否はせず、検証作業だけ行って利用するということになるはずである。

こうして、認証局と証明書取得者の間に証明書利用契約ないし利用約款合意といった関係を擬制するのは、あまりにも形式的に過ぎ、妥当とは思われない。むしろ、両者には直接の契約関係は存在せず、ただ単に、契約の連関が認められることから、必要な範囲で、契約に起因する債権関係の連鎖関係が存在すると見るだけで十分であると考える※5。

ECOM/WGの議論も、依存規約の合理性を指摘するが、あくまでも事業者サイドの

※４CPSの実例　「2.1.4 依存者の義務　　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」日本認証サービス AccreditedSign　Certificate Policy and Certification Practice Statement(V1.51)http://www2.jcsinc.co.jp/repository2/ASignCPS.pdf

※　5 依存規約（リライイングパーティアグリーメント）の存在は認証局の事業参入を容易にし、依存者も電子商取引を利用しやすくなる」ECOM/WG「認証局の責任に関する提言」13頁とするが、依存者が電子商取引を利用しやすくなるかは疑問である。

合理性追求であって、全体としての機能という点から、活用という点からは問題が多すぎると思われる※6。

なお、④成りすまされた者の責任も発生する可能性を否定しきることはできない。たとえば、安易に印鑑証明書などを預けて、電子署名の作成と認証の登録ができるような条件を作り出したような場合には、一定の管理責任が問われる可能性もある。これまで実際の世界でもこうした管理責任を問われたことはほとんどないが、果たしてオンラインでの処理にあたって、そうした高度の管理責任を認められるかは、疑問なしとしない。

なぜなら、他の証明書の権利者（本人）においてオンライン利用を意図していた場合ならばオンラインで発生する危険性の予知、責任の予測が可能であったといえるだろうが、そうではなく、オンラインと無縁の人も存在する。オフラインで生きている人の名義を利用するような場合も考えられる。そのような場合、利用されたものにとっては、まったく予測できず、被害発生は不可抗力に近いものとなる。こうしたときにまで管理責任を認める基礎は存在せず、従ってすべてに対して管理責任を認めることはきわめて困難であると考える。

重要な問題は、事故の発生に関して、どのような賠償義務、責任が相互に発生するか、ということである。

1.1.5. 事故の予測

本考察では、事故内容をさらに詳細に検討したうえで、各当事者に対する適正な責任配分を考察するものである。既に、ECOMによって「電子署名利用者システムの構築・利用ガイドライン」が作成されており、認証局において検討すべき手順の概要が示されている。ここでは大変詳細に、守るべき手順が示され、事故の発生が事前に回避できるようにシステム化されており、一つの理想形が示されている。しかし、このガイドラインそのものが法的責任の切り分けをするものではなく、法的判断はまた別の観点から行うべきものと考える。

※6「認証局の責任に関する提言」ECOM　平成12年3月
「本報告書においては、依存規約（リライイングパーティアグリーメント）を有効にすべきであると　考え方に立っているが、認証書の検証方法についても技術的手段が確立されていない現状において、検討の余地が残されているところであろう。」として、依存規約を基礎におく見解に立っているが、これはあくまでも、クローズドＰＫＩ（登録者も利用者（依存者）もともに同一の証明書の利用者で、同一の認証局を利用しているという場合）において成立する議論であり、本来のPKIシステムではないことに注意が必要であろう。
http://www.ecom.or.jp/report/wg2-2/e11-cn3.pdf

予想される事故

まず発生する可能性のある事故の類型を見てみることにする。

１）誤発行成りすまし事故

まず、誤届け、成りすまし届けなどを元に誤発行がなされ、これにより本人に成りすまし、成りすまし犯人との間で取引が行われるという事故が考えられる。

２）権限逸脱事件

資格、権限など属性証明に関する偽造などによる証明事故

無権限の場合

基本権限からの逸脱

３）発行後流用成りすまし事件

①　離席時成りすまし

②　不正アクセス事故

③　カード紛失と収得後知情意利用事件

４）失効後有効仮想事件

また、発行時には正確な情報に基づいて正当に証明書が発行されたのだが、その後登録者の登録情報が変化して証明書が失効するに至った（存在事実の変更、たとえば死亡、法人解散などの事実にかかわる失効の場合や、有効期限切れで更新がない場合など）ので失効したが、登録者は執行の事実を知りながらこれを利用し、他方で証明書取得者は失効の事実を知らず、発行された証明書を信頼する。その結果、失効した証明書を利用した取引が行われるといった事故が考えられる。

５）失効誤認事故

さらには存在事実に変化はない（死亡、法人解散などがない場合）ものの属性情報の変化（法人破産による権限制限、管理権限・処分権限・代表権の移動など、役員解雇、資格喪失、信用情報変化など）があったがその属性にかかわる被証明者本人がそれを隠して、以前発行された真正な、有効期間内の証明書を利用して取引を行い、取引の相手方は資格などを故意に虚偽表示して、相手方を騙したといった事故が考えられる。

６）システム障害などによる事故

2　証明書をめぐる事件の検討

2.1　判例分析の視点

このような多様な事故にあっても、本来は、行為者そのものが本体とも言うべき契約締結に関する意思表示をしており、それに伴う責任を取るのが本来の姿であって、問題は、契約などの効果を帰属させるべき主体が不明で契約の履行を実現できない場合（成りすまし事故で、主体が判明しないため資金の返還が実現しないなど)､あるいは主体は明確だが無資力などによって契約などの履行を求めることができない場合に大きな損害が発生した場合である。そのような不測の損害が発生した場合に、契約の相手方であり、証明書保持者である者のみがすべて負担する（責任がある）と見るべきなのか、それとも、そうした事故を誘発したもの、関連する落ち度のあったものに何らかの分担、振り分けが必要なのか、を検討することが必要になる。登録のミス、発行のミスに関してはすでに詳細に検討した※7。

ここでは､むしろ､正確に発行された証明書が､何らかの意味合いで濫用され､失効した場合に､法的関係に影響を及ぼすのか､という点を検討することになる。大変興味深いのは、印鑑証明、登記簿謄本、戸籍謄本などが発行された場合に、その誤発行に伴う責任と、正確に発行した後の有効期間内の事実変化に関する現在の責任関係の検討が、従来の仕組みの中でどのように検討されてきたかを見ることである。

2.2　関連判例の検討

2.2.1　基本代理権逸脱

基本代理権を与えたが、証明書の所持者が与えられた権限を逸脱して証明書を濫用して第三者と契約した場合

（平成１１年９月２２日東京地裁民第４部判決（確定）金融商事判例2000・6・1号）

事案　印鑑証明登録名義認であるＸが､正規の証明書の発行を受けた｡Ｘは、

※7 電子認証局の法的責任　２００２年４月１２日　牧野二郎
http://www.asahi-net.or.jp/~vr5j-mkn/BusinessLaw/
http://www.ddtf.jp/data.htm

ダイアルＱ２の登録をＡに依頼し、ＡがＸの代理人となり右登録行為を行うことを承諾してＡに発行済みの印鑑証明書と実印（健康保険証も交付したと考えられる）とを一緒に交付した。Ａは、自らの債務をＸの同意なく、Ｘに連帯保証させようとして、Ｂと共謀して、ＢをＸであると偽り、ＢにＸの健康保険証を保持させ、あたかもＸであるかのように振舞わせ、信用保証協会をしてＢが、あたかもＸであるかのように誤信させ、信用保証協会はＢをＸと誤信し連帯保証契約を締結したという事案である。

なお、証明書の申請行為を問題としたのではなく、ダイアルＱ２の契約を行い、登録を行うことを依頼したことが基礎となり、それに付随して印鑑証明書を交付したという事案であり、印鑑証明書を代理権の存在を示す証拠として濫用したため、Ｘの法的責任を問われたという事案である。

判決　裁判所は、ダイアルＱ２契約を締結する代理権（基本代理権）※8を付与したことを認め、それを基礎として、代理権の範囲を逸脱してもの（基本代理権と逸脱した代理行為との間の食い違いについては問題としないという実務の通例によった）であるとして、こうした逸脱に関して、相手の善意無過失であれば民法110条の類推適用により契約は成立するとし、健康保険証という通常本人しかもっていない証書を持っていたことを信じたことに過失はないと判断して、契約の成立を肯定、Ｘが連帯債務を負うと判断した。

検討　基本代理権があるとき、それを代理人が逸脱した場合の責任は、基本代理権を与えた本人が負うべきだ、というのは民法の通常の理解であることからすれば、当然の結論と見ることができる。

本来基本代理権は法律行為を委任するなど、一定の意思表示をする権限を基礎とする。そのため、行政的な手続きの実行を依頼する場合は、機械的に書類を運ぶという行為になるのみなので、基本代理権にはならない。したがって、印鑑証明書の交付申請行為のみを第三者に依頼しても、そのことだけでは表見代理は成立しないと考えて良い。

しかし、本件のように特定の契約締結行為を第三者に依頼する場合は、ダイアルＱ２契約の締結という契約上の意思表示を行うことを委託し、代理権を授権したのであり、基本代理権限を与えたということができる。

オンラインの場合、認証局への登録申請行為が、認証行為を行うことに

※8 民法１１０条の表見代理においては、基本代理権があり、その範囲を逸脱したことに関して、本人（代理権授権者）に責任が及ぶとしたのであるが、代理権もないところには、権限逸脱はなく、単なる無権限であるとする。権限逸脱について、基本代理権の存在を重視して、取引の安全と静的安全の調整を図っていることがわかる。

関する契約であるのは明らかなので、仮に認証契約を委託した場合、それを逸脱して濫用すれば、認証契約権限を基本代理権とした、表見代理となる可能性もある。

いずれにしても、法的に見れば、第三者に登録を委託した場合に、委託を受けた第三者が預かり書類を濫用して権限逸脱行為を行った場合には、契約の相手方を守るため表見代理が成立することになる。

濫用されるかもしれない代理権限を与え、実印、印鑑証明書、健康保険証などを預けるということは、そうした濫用の危険性まで付与した、と見ることになる。代理権限に対する制限についても同様で、その制限を与えたことをもって善意無過失の第三者に対抗できず、対内的関係で拘束力を持つにとどまるのもまた同じ理由からである。

電子署名の場合、役職者への権限制限、属性認証における属性の制限など、基本代理権限に対する制限は、電子署名・認証証明書において明示されない限り、電子署名取得者に対抗することができないと解されることになるであろう。ここでは、登録者、証明書の名義人が責任を取ることになると思われる。

しかし、仮に電子署名、認証された証明書自体に権限の制限や、権限の範囲などについての情報が明示され、簡単に確認されるように明示されているようなケースがあるとすれば、その制限は有効に告知されていたとして、当該制限を、証明書取得者に対抗できていいのではないか、と思われる。契約自体には制限が明示されていない場合で、証明書だけに制限が明示されている場合に当然に契約権限の制限を対抗できるといってよいかは重大な法的問題である。少なくとも、相手方の過失は認めることができるであろうが、現時点では、証明書の表記内容が明示的で、かつ、極めた簡易な手段で検証できるという条件の下、証明書取得者にはその権限制限を対抗できると考えたい。

2.2.2. 期限切れ証明書の意味

期限切れ証明書を利用し、契約を締結した時の契約の有効性に関する事案

3ヶ月超印鑑証明書による預金払い戻し事件

（平成10年10月29日東京高裁第10民事部判決　金融商事判例1056号14頁）

事案　共同相続の事案で、共同相続人間で、銀行預金債権を相続税支払いに

当てるという合意が成立したが、共同相続人1人がこれを承諾しながら協力せず、印鑑証明書を交付しない。それどころか、自ら印鑑登録を抹消し、有効な証明書を発行できない関係を作った。そこで、他の共同相続人らは、かねて受領済みの印鑑証明書を流用することにして、祖任官証明書を添付して預金債権払い戻し請求を行ったところ、銀行はこれに応じて払い戻し行った。ところが、その時点では印鑑証明書はすでに期限が切れ、さらに3か月経過していた。

判決　印鑑証明書の添付が求められている理由は、本人であること、本人の意思によるものであることを確認するためのものであって、意思確認等に資するには期限の制限は重要ではない。法令に特段の規制がない以上、有効と判断するほかない。金融機関としては、当該文書の作成名義人、本人の意思に関して、疑うに相当な事情がない限り、通常の方法で判断すれば足り、6ヶ月近く経過したものであるということから直ちに過失があるとはいえない。また、本人があらかじめ与えた授権を解消させるのであれば、その旨を告知すれば足り、銀行の払い戻しを停止させる意図であれば、銀行に連絡するなどごく簡単な方法でこれを実現できたのにこれをしなかった。銀行は、特段疑う事情もなかったのであるから、有効な債権の支払い（法的には民法478条債権の準占有者への弁済）として有効である。

検討　印鑑証明書の有効期限に関しては、法令によってさまざまな扱いがある。登記申請においては3ヶ月以内のものであることが求められている（不動産登記法施行細則42条・44条）。これに対し、取締役会議事録に添付すべき取締役の印鑑登録証明書は有効期限の定めがない。また、公証人法28条2項などによる面識のない嘱託人の提出すべき証明書は作成後6ヶ月であることを求めており（昭和24年5月30日民事甲第1282号法務省民事局長通達）、法令によりさまざまに規定がなされている。

判例も言うように、たとえ3ヶ月内のものであっても、怪しいものに対しては再度発行を促すなどの対処が必要となる場合もあるのであって、その期限に左右されるものではない、とされる。この結論もきわめて妥当なものであって、登録者がその都合で失効申請をしたからといって、そのことで、直ちに証明書信頼者の落ち度があるといえるのかどうか、契約が無効になるとすべきか、慎重に検討すべき問題である。

2.2.3. 期限切れ証明書に基づく公正証書の有効性

６ヶ月超印鑑証明書による公正証書作成事件

（　最高裁昭和41年7月26日第三小法廷判決　金融判例　No１８　7頁　）

事案　公正証書を作成する場合には、原則として6ヶ月以内のものでなければならないことは民事局長通達によって示されていたが、本件では提出を受けた印鑑証明書は作成・発行後6ヶ月を超過したものであり、作成された公正証書に基づいて強制執行が行われたため、債務者が公正証書の有効性を争った事件である。

判決　公正証書の作成経過が所定のものであっても、作成過程の諸般の事情の下では公正証書は有効である旨の原審の判断は正当である。

（原審である仙台高裁、第一審である青森地裁もともに、債務の有効な存在、公正証書作成に関する代理権限などの作成過程に関する事実関係についてすべて有効であることを前提に、いわば形式違法である有効期間問題に関しては公正証書本体の実質的有効性を左右するものではない、と判断していた）

検討　この事案は、明らかに法令に反する資料を提出したものであって、形式的には印鑑証明書の利用は違法となる事案である。しかし、参考資料の1つが有効期限を徒過していたとしても、他の事情や関連資料などから、公正証書自体の成立を左右するような事情がない場合には、こうした軽微な違法を問題とする必要はないというのは常識的範囲の問題であろう。

したがって、証明書の有効期限切れなどに関しても、その有効期限の意味が形式的なものである限り、契約自体の有効性を左右するものと考えずに、実態を考慮することで有効と判断される可能性が高いと考えられる。

ただし、この事例も期間制限徒過という問題であって、実質的に権限を喪失し、失格になった場合ではない。今後属性認証の失権が登録されるような場合には、その登録を確認しなかったような場合に重大な落ち度とされる可能性はある。

これまでの判例は、すべて実質的には有効であるという前提で、形式的違法を持って実態を否定することはできないといった判断をしたというべきであって、無理な拡張解釈は避けるべきであろう。

2.2.4. 判例のまとめ

これまでの従来の社会での証明書をめぐる判例は、おおむね次のようにまとめることができる。

まず、証明書の持つ効力、信頼という機能の点では、裁判所は、その効力を積極的に認めている。すなわち印鑑証明書などが存在することは、法律行為を委任したこと、すなわち法的に代理権を授与したと認定する材料となる。少なくとも、そうした基礎になる権限授与があるという前提で、それを逸脱した場

合には、証明書の持つ外形的信頼を基礎に、相当広範囲の法律行為に関してまで効力を及ぼすという判断になる。こうして、裁判所は、証明書が濫用されて外形作出に影響力を持つ限りは、そしてそのように利用されたことに関しては、表示した外形、濫用された外形に沿った責任を肯定するも、証明書の効力に特別な意味を認めていないのはその他の判例でも明らかである。

他方で、証明書の証明期限、発行後の有効性という点であるが、比較的緩やかに認識され、過去の事実を証明していることに重きを置いて、形式的手続きの違背に関し重大視しないということができる。こうした観点からは、証明書は、あくまでもある事実の証明書に過ぎず、他の方法でその事実の存在が証明される限りは、証明書の期間徒過等は重要ではないのは常識的判断と一致する。

2.3. オンライン証明の特殊性

もともと一般常識的にも、証明書というものは証明書の発行日時を明示して、その日時のものとして証明行為を行うものである。その発行時点での存在証明をしているだけであって、有効期間内の間中、その事実が存在するということを保証するものではない[※9]。証明書が正式に発行されている以上、それを信頼するとしても、完全な信頼ではなく、それをさらに最終的に補完するといった最終検証手段（登記登録の実施、金融機関による金融情報や有価証券のチェック、同時履行の確保、担保権設定など）を併用することが多い。従って、この点から、有効期間中の失効による事故に関する責任は、認証局には存在しないという方向、すなわち、他の手段を併用するなど、証明書保持者と登録者（被証明者）との間で処理する、という現実的運用がなされているといえる。

そうであれば、電子署名においても、現実の社会運用と同様な基本方針を持つという見解も存在するだろう。すなわち証明書・認証に関しては、これを本人が積極的に利用した場合にはその外形に従った処理がなされるとしても、認証局は、証明書の期限切れや、証明期間における事情変更、登録事項変更に関して、その不存在（不変更）まで保障したものではないとし、従って、発行時期における事実関係の証明という範囲を超えて法的責任を負うものではない、という考え方もできる。

しかし、自律的手段が多様に用意されたリアルワールドでは確かにそうであるが、果たしてそうした手段の用意されていないオンラインでの証明行為においても同様といえるのか、慎重な検討が必要である。

※9 登記簿謄本も証明の時点（瞬間）での内容を反映するだけで、同日に権利移転があるとしても、その移転を否定するものではない。印鑑証明・住民票も同様である。

2.4. 従来の制度との重要な違い

オンラインでの証明書の存在は、オンラインでしか確認できないことに最大の特徴がある。またそれがオンライン証明書の目的でもある。リアルワールドでは、証明書を検討するための、あるいは事実関係を確認するための他の多重的な手段が多数存在し、現実に機能している。

しかし、オンラインではすべてがデジタルデータとして、電気回線を通過するのであって、遠隔地相互の取引にあっては簡単には相手方を確認することができず、利用者はオンラインでの証明を信頼するほかない。こうした観点からは、オンラインでの証明は少なくともリアルワールドでの信頼性と同等かそれ以上の信頼性を確保すべきであるが、実は、オンラインでの証明の検証はオンラインでしかできないのであるから、証明の真実性に関しては、二重、三重の検証手段が与えられるべきである。そうした証明書の確かさ、すなわちリアルな社会での各種の検証システムに匹敵するような、あるいはそれ以上の総体としての信頼性が確保される必要がある。

こうした考えに対しては、リアルで違法なものはオンラインでも違法、リアルで期待できないものをオンラインで期待することはできない、オンラインは絶対でないのだから、リアルと同じ程度の信頼でよいはずだ、との反論も考えられる。しかし、リアルな動作とオンラインでの動作の決定的な違いは、リアルな動作は計算しきれない複雑さをもった実在として存在するが、オンラインでの存在は０と１の信号としての存在でしかないという事実であり、こうしたデジタルデータはいったん作られると他の諸関係から切り離され、独立して、孤立してデータとして転々としてしまうものであること※10、従って、データが他の諸関係と関連付けられるという意図的な仕組みができない限り、実のところ、リアルワールドとは等価にならない、という点である。

データの世界で重要なものの一つが「リンク」である。データは、諸関係から切り離されやすいので、加工しやすく、流通にも適している。その特性、長所は、実は自己の存在を示し、位置関係を示す上での最大の欠陥、短所となっているのである。その欠点を補うものがまさにデータ相互を関連付ける「リンク」なのである※11。

※10 書籍などは、出版社が実在し、書店という実在と関連付けられ、さらに図書館や大学に実在するなど、書籍としての実態が見える。それを通して、著者の評価、社会的位置、社会の取り扱いが見える。しかし、オンラインの論文などの場合は関連性が見えず、情報のみが孤立していることが多く、社会的評価も、信頼性も希薄となるという実態がある。

※11 リンクは、情報相互を関連付け、位置関係を示す機能を持ち、マッピングするための重要な役割を果たす。リンクのないデータは、利用することが困難で、社会的利用されることも少なくなる。その意味で、データにとってリンクは生命線ということができる。

オンラインで利用される証明書は、証明書単体ではなく、常に認証局の認証と一体化しなければならない。そしてその認証された証明書は認証局にリンクされているべきである。その証明をした認証局はさらにその認証局の存在を支える上位のルート認証局へリンクされなければならない。こうした連関があること、」そしてこのルートが保障され、証明書の正確性が保障され、利用者が容易に検証できる仕組みがあって証明書データは安心して利用できるものとなるのである。こうした保証の連鎖があることで、電子署名は信頼される価値のあるデータとなるのである。この考えに立つとき、オンラインでの証明書に対しては十分な保障と検証の手段が与えられていなければならないと考えるべきである。※12

では具体的にどのような関連付け、さらには検証方法が必要になるのか。

2.5. 登録確認・有効性検証の対象

ここで重要なのは、オンラインの証明書の信頼性に関して、合理性、利便性とのバランスを図ることである。仮に、信頼性を高めるという目的だけであれば、あらゆるところで、アンカーを置き、現実社会と関連付け、基礎付けることができる。しかし、それではオンラインで処理できるという利便性を大幅に失うことになる。従って、オンラインの利便性を減殺することなく、かつ、信頼性を確保する方策、仕組みが重要になる。

まず、電子商取引における信頼性は、端的に言えば、当事者として確定できること（訴訟提起が可能であること)、支払いが確保できること（支払い保証、担保などの存在）である。従って、この範囲で情報が正確に提供され、確認できれば良いことになる。極端に言えば、本人性や、本人の実在、存在は必須ではない。むしろ支払い確保が確実であれば、実在性すら不要である。これはプリペイドカードによる決済方法や、法人という擬制組織の行動を認める仕組みが既に立証しているといってよい。従って、究極には架空人であっても、口座を持ち、口座の資金決済の権限を持っていることを口座を管理する機関（銀行など）が証明しているときは、その架空人との間の取引は有効であるし、回収の確実性も確保されており、結局信頼されることになる。こうした場面では、本人性やその実在はまったく意味を持たないことになる※13。電子商取引に限っていえば、支払保証が最大の信頼であり、二次的に当事者の確定が信頼の基礎

※12 ここでは、通常の使用例とは異なるが、リンクはデジタル情報相互の関連性、アンカーはリアルな社会との接点の確保の方法、を意味するものとして使用する。

※13 口座に現金や、オンライン送金で預金し、預金を確認した場合に預金権限者であることを証明する電子署名・電子証明書を銀行が発行する仕組みを考えれば、その電子証明書があたかも人の証明のように機能することになる。これは、銀行の自己宛小切手（預金小切手）と呼ばれる仕組みで、現金同様に流通し、これをオンラインで利用できれば、電子商取引は活性化すること間違えない。

となる。

これに対して、行政手続や各種証明手続きなどにおいては実態としての存在証明が必要となると考えられる。また、口座開設の契約にあっては、契約の前提として、支払い確保などとは別の要請、すなわちマネーロンダリング防止などの政策から必要とされることがある。こうした場合はむしろ刑事事件として処理するという観点から、実体としての存在との関連を必要とする。

この観点からは、本来は支払能力や資格などを問題とする属性証明は、必ずしも、存在証明（本人性）と結びつくものではなく、本来は別の制度として機能しているものである。しかし、電子商取引も、その他の作用も、最終的には刑事的な処分や責任追及という厳格な責任追及を背景に持つ可能性が高く、その場合には属性証明が存在証明と強く関係付けられることになる※14。

3. 電子署名に関する事故と責任の検討

3.1 責任の前提

電子商取引が実現せず、何らかの障害に遭遇したときには、履行責任、賠償責任をめぐり、責任の追及がなされることになる。そのときは当然に電子署名、その認証に関する責任も問題とされる。契約履行という面での信頼が阻害されたのであるから、証明し、認証したものの責任を問うことになるのである。そのためには、次のすべての条件が満たされなければならない。

まず、①証明書の誤発行ないし証明書の失効という客観的事実その存在、次に②として、①の事実に関する責任者の故意、落ち度など責任を帰するための責任帰属要件の存在、さらに、③として利用者に現実の損害が発生しているという事実、④として以上①ないし③のすべてが合理的な相関関係にあること、などがすべて検討され、責任の要件が満たされる必要がある。

こうして条件のすべてを検討して、損害賠償責任が認められることになるが、損賠償額、責任の範囲はさらに慎重な検討を要することになる。当事者間の責任の割り振り、落ち度の大小、その他損害を拡大することへの寄与の程度など、さまざまな関係から、責任の配分（過失相殺）をすることになる。その際、証明書取得者（信頼者）の証明書の検証行為の有無、難易度、仕組みの簡便さなどが重要なファクターとなるものと思われる。

※14 電子署名及び認証業務に関する法律　6条1項2号「申請に係る業務における利用者の真偽の確認が主務省令で定める方法により行われるものであること」とされ、利用者の真偽に対する監督がなされることになっている。

3.2　賠償額の際限なき拡大と「正当な信頼」の原則

現実の損害は、証明書を利用することで可能となった取引に基づいて発生したもの全額に及ぶ可能性もあり、現実的社会でのトラブルよりも広範に発生し、拡大する危険もある。間違えて発行した証明書が、犯人の犯行を覆い隠すために悪用され、全世界の不特定多数のものに利用され、その全世界の数十万人ものすべての利用者に損害が発生したような場合で、証明書の誤発行や失効に関して、認証局などに故意、過失などの責任要素があった場合、認証局に天文学的数字に及ぶ損害賠償の責任が発生することも考えられる。

こうした認証局の過失などにより、認証局が広範囲に広がる責任を負担する危険に対して、その責任の範囲をあらかじめ制限する主張がなされ、合理性があるとの強い見解が点されている※15。

その根拠は、電気通信事業者同様なインフラ整備であること、99年ＥＵ指令の採用する考えであること、さらに実質的には認証局の事業基盤の圧迫、利用コストの高騰などを理由とする。

しかし、電話回線の場合は「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。」（電子認証局の法的責任牧野）と指摘したとおり、認証局の行っている作業は単純なインフラ提供にとどまらない。その上のサービスとしての信頼の普及行為である。印鑑証明書の発行以上の、重要な基幹産業なのである。現実社会で印鑑証明書の誤発行に関して、各地方自治体が責任を取っている事実については既に検討したとおりであり、電話回線事業との違いは明確になっていると思われる。これが、既に述べた「正当な信頼」の理論である。

また、事業基盤圧迫という指摘には、そもそも責任限定という形で、無責任体制を採用することで信頼が確保されないときには、産業自体が発展しないこと、従って、事業を圧迫させるような広がりさえ発生しにこと、目の前の責任回避をすることで、認証事業全体を信頼されない無用の長物にする議論になりかねない点を考慮しなければならない。

責任限定は、普及の段階で、損害の過度の負担の派生した時点で検討すれ

※15 「認証局の責任に関する提言」ECOM/WG　12頁　同45頁

ばよいことであって、あまりに強いリスクヘッジは産業自体への圧迫となる。そもそも、保護されるべき信頼の範囲を、ＣＲＬを確認したもの、ＯＣＰＳによる確認を行ったものと限定し、そうした作業をしないものに対して利用者の過失を認める制度とすることで、より信頼性が高く、合理性のある仕組みができるのである。

責任を限定し、取るべき責任を取らないという選択ではなく、信頼された保護すべきものはすべて保護し責任を取る、その範囲は利用者のなすべき作業を前提とするという仕組みを採用すべきである。

ところが、提言の立場に従って、広範な拡大の可能性があるオンライン取引の場合に、その損害額の拡大を恐れて、認証局の責任を回避する対策が用いられ、損害額の上限を定め、あるいは総額を制限するといった内容のＣＰＳが多数存在する※16。こうした対策は、利用者の被害を放置し、その犠牲の元で認証局だけが救われようとしているものであって、こうした対策はかえって証明書の信頼性を損なう仕組みとなる。こうした損害の際限なき拡大の危険性の中で守るべきことは、証明書利用者の「正当な信頼」を守ることであって、「正当な信頼」を尊重し、守りきることが認証局の全うすべき責任であろう。「正当な信頼」とは、証明書取得者に対して求められる勤勉な対応、すなわち証明書の確認、検証行為であり、これを履行した場合には、証明書取得者の証明書の有効性に対する期待は合理性があるものとして保護されるべきである。証明書を取得したものが、その証明書の確認を行うことによって容易に信実を確認できる仕組みをとり、その簡単な検証手続きを実行したもののみを守るという仕組みを確立することが必要なのである。簡単な検証行為すらしないものは、守られるべき「正当な信頼」を持つものではない、ということができるのである。

以下、発生すると考えられる事故に応じて問題点を検討することとする。

3.3　証明書誤発行事故

何らかの理由で認証局の署名に対する証明書が誤発行され、その証明書が利用されたことによって、取引の相手方に損害を与えたという事案が考えられる。

まず、この類型にあたる場合というのは、事故発生まで、容易にわからない、発見されないという特徴がある。偶然発見されることも否定しないが、誤発行自体は、通常検査する方法が考えにくく、それを避けるには多様な検

※16 ＣＰＳ比較表　参照

討が必要となる。

そうした段階になるまでは、認証局が責任を負担すべきものと考える。

3.4. 受理時点でのミス（責任の前段階としての落ち度の存在）

3.4.1. 登録者の故意による虚偽申請（認証局がだまされて登録）

登録者の虚偽内容の申告を、登録局において正しい申告と認識して、登録をしてしまった場合であるが、登録申請者が正確でない申告内容によって自らが何らかの利益を得ようとしたか、あるいは第三者（登録名義人）に義務を負担させようと考えた場合などに発生すると考えられる。

登録局のミスは、通常の注意力によって認識できる程度の登録申請の内容の齟齬、不自然さなどを不注意によって見逃した点にある。こうした明確な場合には認証局の責任を肯定してよい。

但し、こうしたミスが存在していても、現実の契約、履行行為の中でそのミス、間違えが発見され、是正され、あるいは事実上訂正されて運用された場合には、実害は発生しないことになる。そうした場合には、後に述べる責任の問題とはならないと考えられる。

3.4.2 登録者による正規申請を誤って認識し、誤ったまま登録

登録申請者が正しい登録申請をしたが､誤って登録した場合｡具体的には、申請とは異なる氏名を間違えて登録したとか、職業を間違えて登録したなど、後に利用（悪用）されるような間違えをした場合が考えられる。こうした場合、通常は申請人が事実に反することを発見して、登録局に申告するのが契約上の務めであるが，これに反して悪用することが考えられる。悪用の形態は、通常の成りすましなどと基本的には変わらない。

こうした場合は、認証局と登録者の共同の過失、過失の共存という現象が生じるが、こうした過失責任を利用者に転嫁することはできない。

3.5. 認証局の責任

だまされたことに過失がある場合には認証局が責任を負うべきであり、その損害の範囲に限定はないというべきである。

すでに「認証局の法的責任」において検討したように、明確な過失の場合や、通常要求されるべき程度の注意義務を果たしていない場合には、過失責任を負担することになるというべきである。

ただ、どこまでの注意義務を負うか、については微妙である。一般に電子署名の際は、提出される書類は公的機関の発行した正式な証明書、関係書類であるため、それらの成立を客観的に検討することで足りるはずである。発

行に当たって、所定の確認作業、所定の手続きを経ておれば、それ以上に照会、比較検討すべきものは存在しないため、注意義務は尽くされたというべきであろう※17。

間違えた証明書発行がなされた場合でも、その間違えが、事前に、すなわち損害賠償の発生する事件発生前に発見されるのかといえば、きわめて困難である。虚偽の証明書や成りすましの証明書を悪用し、発覚しないように工夫されるのが通常であろうから、容易には発覚しないというべきである。したがって、権利喪失にかかわる「失効情報リスト　CRL」に載る可能性は低く、事故発生の事実の予見も対応も極めて困難である。

しかし、認証局は虚偽事実の発生防止のため、最善の努力をしなければならない。まず、登録者の成りすましを防止するために証明書の送達方法として、直接本人に交付するか、『本人限定受け取り郵便』の制度を利用して、これを正確にしなければならない法的義務があるというべきである。これは認証サービス契約のもつ本来の契約上の義務であると同時に、電子認証法の要請であるといってよい。

次に、認証局は登録者本人に、証明内容の再確認を要求しなければならない。認証局のサービスは、契約上の２当事者間の自由な契約に尽きるのではなく、インフラの適正活用という側面も持つ。従って、認証局は登録者の主観的要求に拘束されず、客観的に正確な証明書であることを客観的条件と照らして確認すること、客観的事実との合致を確認するよう要求し、かつ履行されていることを確認することが必要となる。

3.6.　認証局が間違えを発見したときの処理

何らかの理由で、認証局が登録事項や証明事項の間違えを発見した場合には、認証局は直ちに失効情報リスト（ＣＲＬ）に掲載する必要がある。載せることで、事故が発生しないわけではないが、勤勉な証明書取得者（信頼者）が、自ら行う検証行為によって、問題を発見し、保護されることになる。失効リストに載せることで、保護すべき信頼が害されることから守れたにもかかわらず、これを放置することにより、損害が発生してしまった場合には、その損害に対して、責任をとるべき問題となるものと思われる。

3.7.　登録者・被証明者の責任

オンラインで利用する証明書であっても､現実社会とのリンクを重視して、

※17　電子認証局の法的責任　牧野　判例検討を参照

現実の社会の証明書を基礎とし、そこで発行された証明書に立脚し、かつ、現実に本人であることを確認して証明書を交付することが予定されている。一時期郵便で郵送することも提案されたが、その不確実性を理由に「本人限定受け取り郵便」という新しい制度が創設され、本人に直接交付する方法として利用されるに至った。

こうして、証明書は本人に確実に交付されることになったといえ、ここに現実とのリンク、照合が可能になった。従って、証明書の誤発行に関しての第一段階のチェックは、登録者本人の確認行為を上げることができる。登録者本人は、その証明書の内容を確認し、内容の齟齬がないこと確認することになる。仮に、第三者が成りすまして申請したとしても、通常は本人に手交され、あるいは厳格に郵送されるのであって、この時点で成りすましの防止効果が格段に向上することになった。

次に内容の齟齬や、失効に関してはどうか。こうした内容に関しても本人自身が確認する義務を負担するはずである。認証局との間で締結された契約関係によって契約上の義務として存在するのであるが、同時に、証明書を交付する契約の相手方、すなわち証明書取得者・信頼者との関係でも契約上の責任を負うことになる。従って、登録者の証明書確認義務の不履行は、認証局に対する不履行責任を負うとともに、証明書所有者に対しても負うことを意味する。

3.8. 証明書利用者の責任

証明書取得者の注意義務

まず、証明書を受け取ったものにおいて、その証明書の有効性を確認する義務があるか、という問題であるが、仮にこれを肯定したとしても、本件のような成りすまし登録事故、登録、発行ミスの場合で、かつ、発覚前の事案においては、証明書確認を行ったとしても、検証を義務付ける合理的根拠はない。すでに述べたように、CRLに記載されるのは、届出や有効期限切れなど、ごく例外的な場合に限られる。したがって、誤発行の場合で、その過誤が発覚していない場合に注意深く検証させる意味はない。

しかし、証明書の期限切れや、発覚した誤発行、内容の齟齬した証明書など、あるいは権利が失効した（公的権利剥奪や資格喪失、権利登録抹消など）ため失効した事が明確になった証明書などの場合には、失効届けが重要な意味を持つことになる。

ここから、証明書利用者（依存者）に対して、検証の義務を認める見解もあり、また、検証を義務付けるＣＰＳも多い。

しかし、この義務を尽くさないときに何らかの法的責任を負うか、という

観点から見たとき基本的に法的責任を負うとは思われない。証明書の検証は、単に証明内容を確認するためだけであり、確認する、しないは証明書所持者（信頼者）の自由でなければならない。確認したとしても特別な利益があるわけではなく、単に当該証明書の正確性が確認できただけである。

証明書取得者（信頼者）に失効情報リストＣＲＬ確認義務を認める意味は低く、これを義務とするのは問題ではないかと思われる。しかし、だからといって、検証の意味、必要性がいささかも減少するわけではない。証明書の検証は、「保護されるべき信頼」（前記16頁参照）であると判断するための重要なメルクマールとして機能するのであり、その意味は大きい。

3.9. 人違い発行のミス

ＡとBとの同時の申請を受けた認証局が、同時に証明書を発行したが、証明書（秘密鍵と公開鍵認証証明書）を間違えて取り違え、Aに対してBの証明書を、Bに対してAの証明書を発行するというミスが考えられる。

明らかに認証局の責任であり、これに対する責任がすべて、全額認証局が負うべきものである。

4. 失効に関する問題

4.1. 登録時は正確であったことの評価

基本的に登録時正確な情報を登録したので、登録時における登録局の登録ミス・発行ミスはないはずである。認証局は、申請者の申請どおりに正確に登録し、認証したのであって、この時点での証明・認証は正確であり、なんら登録局には責任は発生しない。

しかし、その後、何らかの事故（死亡、戸籍上の姓・名の変更、法人解散、法人破産、法人合併による消滅など）により人格の喪失ないし大幅な地位、属性など事実変更の発生による証明事実との齟齬が生じた場合に、どのような変化が生じるのか検討を要する。

そもそも、この登録事実との齟齬についても、変更事実発生と同時に自動的に直ちにその変更が反映されるものではなく、登録者ないしその関係者、利害関係人による申告を待って、失効が登録される。ワンタイムパスのようなもので、地位や資格の確認の度に発行するような場合は別として、一般の証明では、証明時の事実関係を証明するに過ぎないといわれる。

ＯＣＳＰ（(Online Certificate Status Protocol ）にしても現在の真正性、登録事項の現在のありのままを知らせる仕組みではないとされ、現在の権利関係を反映するものではないことを前提にしなければならないと

いわれる※18。

従って、現実の失効から失効届けがなされるまでのタイムラグ、さらに失効登録申請ないし、失効届けの後、認証局において失効登録、失効情報公開がなされるまでのタイムラグもある。ＣＲＬの更新の頻度が、１ヶ月などというものであれば、失効したとしてもその後１ヶ月は有効として取り扱われることになる。こうしたタイムラグは、思いのほか大きいものと考えられる（図２参照)。

失効の場合の処理・流れ図

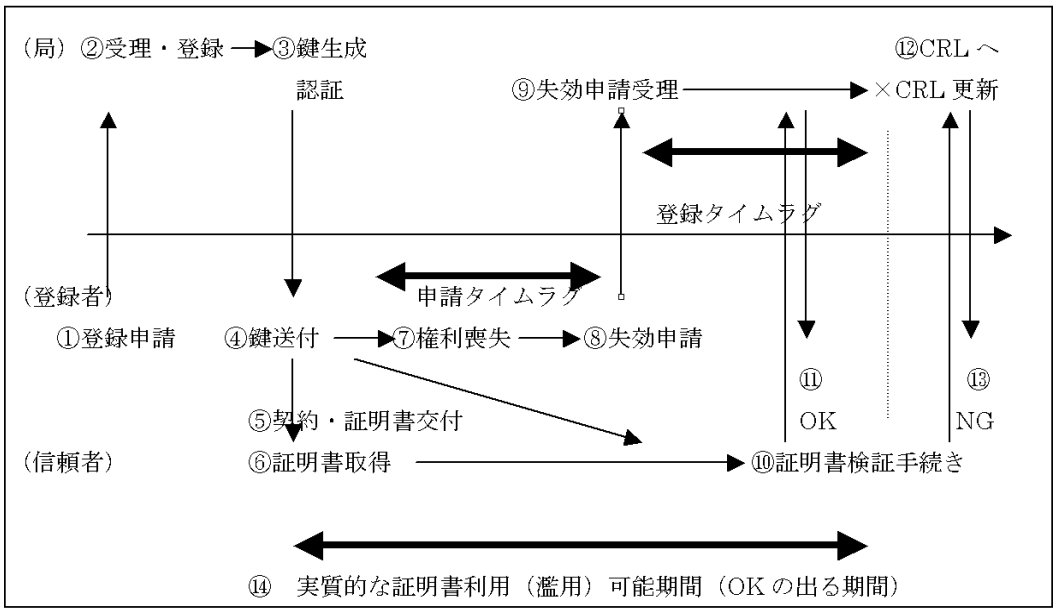

図２

このタイムラグに関しては、きわめて困難な問題となる。失効事実の発生・発見から、失効登録申請までのタイムラグは、登録者ないし承継人の管理範囲といえるが、果たしてその間のトラブルの全責任を負担させてよいかは疑問である。同様に、申請後公開までのタイムラグは認証局の問題ではあるが、現実的に作業の進行自体に時間が必要である以上、全責任を認証局に負担させることも困難である。

しかし、だからといって、すべてを利用者（依存者）の責任とリスク負担でよいとするのは乱暴に過ぎよう。この点、ECOM/認証・公証WGの見解は、

※18 オンライン失効情報問合わせ（OCSP）エントラス鈴木優一　参照

「認証局は、タイムラグが生じることを依存規約に盛り込むことにより、依存者に注意を喚起することが可能であるが、・・・依存規約により免責されるかは問題のあるところである。」として回答を出していない（ECOM/WG「提言」30頁）。

タイムラグについて、認証局などの免責を認めるということは、利用者にすべて負担させるということである。こうした判断は基本的に方向性を誤っていると考える。こうしたリスクは事業者が負担すべきであって、そうすることによって利用者には不測の損害がないという安心感を与えることができるのである。

従って、原則的に認証局が責任を負担し、それでも耐えうるような技術的対応策、登録者に対する義務付け、利用者の検証システムの完備などを優先して、あらかじめこうした方向でのリスクヘッジを図るべきである。証明書利用者（依存者）にリスクを転嫁し、逃げるという形での間違えたリスクヘッジは避けるべきである。

4.2. 失効者、登録事項変更にかかる責任の所在

4.2.1. 登録者の届出責任

登録者が死亡して相続が発生したような場合に、相続人は当該証明書の失効手続きをする法的義務があるのだろうか。法人の管財人、合併後の存続会社の責任者は消滅した企業の関係する証明書について何らかの作業失効届けをする法的義務を負うのだろうか。

またさらには、属性の変化して、従来の証明事項に変化を生じた場合、登録者はその変更を届け出る法的義務を負うかの問題である。

いずれの場合にも、認証局・証明局との間で締結されているはずの、電子認証契約に関して言えば、契約上の届出義務が存在することは容易に肯定できる。また、多くの契約約款、ＣＰＳなどはその規定を置くようである。こうした契約上の責任は、登録申請者と登録局との間の契約上の問題であって、原則的に第三者に影響は及ぼさない。

4.2.2. 第三者に対する責任

認証局に対する契約上の責任とは別に、特定の第三者に対して証明書の有効であった時点で発行された場合、あるいは将来何らかの理由で発行される可能性のある証明書を、登録事項の変化に従って失効させるべく、届出をする法的義務があるのか、の問題である。通常、証明登録者は発行され受領した証明書を自己の表示として使うことになるが、この場合契約の相手方である証明書取得者（信頼者）に対して契約に基づき、契約の履行行為の一環と

して交付するのが通常であろう。そうした行為は、契約の履行の一部であって相手をだましてはならないという誠実の原則によって守られる行為なのである。

なお、これと関連して、ひとたび、失効登録を済ませた登録者は、仮にそれまでの幾つかの証明書を発行していたとしても、その失効情報登録の時点をもって、効果帰属を否定することすなわち、それ以降は証明書を無効なものとして取り扱って良いといったような関係に立つと考えることにも合理性があるといえるだろう。

この点では、証明書取得者は、その証明書の有効な存在を確認するために、失効確認をすべき地位にあると考えることで、仮に予定通り失効確認をしておれば、失効した事実を確認することができ、更なる被害発生や契約の遂行を停止することが可能となったとも考えられる。こうして、きわめて例外的に損害の停止、拡大停止のための勤勉な努力としての失効登録が、損害賠償の過失相殺の際に考慮される可能性はあるといえる。

4.3. 証明書の有効性が問題となる場合

契約をした際に送信交付された証明書が有効であり、あるいは無効になったはずの証明書を送信交付した場合などに、その証明書の有効性が個別に問題となるケースがあるか、である。しかし、そもそも証明書の送信交付は、意思表示の信頼性を確保するための補充手段に過ぎず、そのことが契約の有効性を左右するものではないはずである。

法的観点から検討した場合、この問題は比較的単純であるといっていい。すなわち、意思表示そのものの効果と証明書の持つ効果とは質的に異なるということが問題の区分を明確にする。意思表示は証明書が付くか、付かないかは問わず、本人の意思表示であれば本人に帰属するのであって、本人死亡後はいかなる理由があっても本人の意思表示は存在せず、本人の意思表示として何らかの効果が帰属することもないのである。認証・証明書の存在は、その意思表示の主体を確認するためだけであって、意思表示の根拠とはならない。

相続が発生したり、法人の承継が発生したとしても、権利や義務の承継の有無、効果の帰属の可否などはすべて通常の民事法の原則によって処理されることになる。

4.4. 承継人の責任

登録者としての地位を承継したものは、どのような法的責任を負うのであ

ろうか。登録者の地位を承継したものは、当然のことながら、認証局との間で締結された認証契約の契約上の地位を承継することになるため、権利の喪失などに伴う失効登録申請を行うべき法的義務、契約上の責任を承継することになる。

4.5. 認証局の責任

4.5.1. 正確な登録情報確保の義務

一般的な社会的責任、あるいは法的責任として、一般公衆に対して、正確性確保の法的義務を肯定することは可能であろうか。

法的な意味での義務を肯定するには契約上の合意があるか、あるいは、法的に一定の拘束力を与えるような立法の場合に限定されるものであろう。認証局は、私的業務を行うものではあるが、その中の特定認証事業をおこなう事業者（特定認証事業者）には、電子署名法によって、主務政令に従う義務があり、行政指導を強く受け、的確な情報の安全確保の必要性が肯定されている。

こうした観点から見るとき、電子認証局には通常の私企業の契約上の責任に尽きる事業者の立場とは異なり、信頼という高度な正確性を担保すべき特殊な立場があるものといえ、こうした観点からは、正確性を確保する法的義務があると考えられるだろう。この義務は、広く公衆に対して負うべきものであると考える。現在のところ、こうした認証局は、当たり前のようにＣＰ，ＣＰＳを公開するとし、公開されたものを基本に監査が行われるものとされている。私的企業であればこうした公開は行われず、公的に議論されることもない。公開し、公開した内容に沿って監査するという姿勢には、こうした法的義務を前提におくべきであるとの実質判断があったと見ることができる。

そう考えない限り、ＣＰ、ＣＰＳ公開の義務は出てこないのではないだろうか。

4.5.2. 正確な失効情報提供の義務

正確なＣＲＬを提供することは、認証制度の信頼性を確保するうえで重要な条件であるということができる。認証局が認識できた場合には、たとえ登録者の申請がないという場合においても、正確な事実登録とすべく、失効情報を整備して、提供すべきである。

では、認証局には失効情報提供の法的義務があるのであろうか。すなわち、ＣＲＬを的確に提供する法律上の責任があるか、である。私は認証局に法的責任が存在するものと解する。まず、認証局は登録申請者に対して、申請ど

おりの正確に登録し、かつ証明書を発行する義務を、契約上の責任として負担する。次に、認証局は、不特定の第三者に対して、当該証明書の正確性を担保すべき地位にあり、法的な責任があるというべきである。その法的根拠としては、まず、証明書の信頼性を確保するために当然払うべき注意であることから、条理上の責任として不特定多数人を対象として、法的責任を肯定することもできるだろう※19。

また、当然失効登録ができるのに怠慢で登録しなかったような場合には過失責任を根拠とした不法行為責任を追求することも可能である。また、認証局・登録局は、登録者に対して正確を期する契約上の責任があり、さらに登録者は信頼者との間の契約に基づき、正確な証明書を交付する契約上の義務があり、従って、証明書取得者と認証局は、債権者代位に準じて、正確な情報提供の契約上の義務を肯定することができると解することも可能である。

利用者に、具体的請求権があるのかについては、認証局に正確な証明書を発行する法的義務があるからといって、直ちに反射利益として請求権が発生するとも思えない。具体的請求権の有無はさらに検討すべきだろう。

4.6. 証明書取得者に証明書検証義務があるのか

証明書を取得した証明書信頼者の証明書利用時の検証義務の有無も問題となる。証明書取得者は、その契約に添付された証明書を検証する義務があるのであろうか。失効のリスクを自ら負担するとなれば、そのつど検証することまで求めることは不要とも考えられる。

多くのＣＰＳは、証明書取得者に対して、検証義務を定める※20。

また、ＥＣＯＭがまとめた電子商取引に関する準則でも同様の提言がなされている。

しかし、証明書取得者は、当該証明書を信頼することも、信頼しないことも自由のはずであって、また、当該証明書を発行した認証局とは何ら直接的な契約関係も存在しないのは明らかで、契約責任を認めることはできない。この点、前記準則は、証明書を確認し、あるいはＣＰＳを承諾して証明書を取得すると擬制しているようであるが疑問である。証明書は、登録者が交付するものであって、取得者・信頼者が選択権を行使することはできない。偶然取得するに至

※19 Nifty判決 ニフティ・思想フォーラム名誉既存事件 東京地裁平成９年５月２６日判決
条理による法的責任を肯定した判決

※20 日本認証サービス 2.1.4 (2) 「電子署名の検証など、証明書を利用する際には有効性確認を行わなければならない。」
総務省認証局 CP/CPS 4.4.10 「証明書検証者は・・・有効性を確認しなければならない」

るのであって、ＣＰＳを承諾するか否かは問題とならない。証明書の確認のため、公開されたＣＲＬを確認することがあったとしても、それ以上の合意もなければ、約款や運用規則を承諾するという意図もないのが通常である。

これと関連して、証明書の中にＣＰＳの所在を示すＵＲＬを記載することができるが、これはあくまでも照会することに意味があるのであって、承諾を避ければ利用してはならないという意味まで読み込むことは困難である。

こうして、証明書取得者・信頼者は、検証をすることができるが、法的な義務とはならないと考える。ただ、証明書取得者・信頼者は、検証をしないことの不利益を負担するという意味での検証の責任、検証すべき地位を有するとすることは矛盾ではない。検証しないことで不利益をこうむった場合に、回避できたのに回避しなかったことの責任、注意義務違反は、過失相殺の１要因として考慮されることになる。

こうした意味での確認義務・注意義務を肯定するためには次の要件が必要となる。

１）検証可能であること
２）検証が容易であること
３）当時確認することが、当該取得者に求めえたこと

といった条件は必須であろう。

今後更に検討すべき問題は多数存在するように思われる。その重要なものをあげれば以下のとおりである。さらに議論をしたいと考えている。

１　公的認証の証明責任
２　個人認証と属性認証との関係
３　ＣＰＳの法的位置づけ、法的拘束力の及ぶ範囲
４　ＣＰＳに対する法的規制　RFCの位置づけ
５　電子証明書の保管形態と証拠保全
６　電子署名の証拠としての取り扱い方法、提出方法、評価基準
７　電子商取引分野におけるＡＤＲの必要と可能性

資料とリンク先

「電子商取引等に関する準則」

産業構造審議会情報経済分科会ルール整備小委員会

http://www.meti.go.jp/topic/data/e20329bj.html

「認証局の責任に関する提言」　ECOM/認証公証WG　H12.3

http://www.ecom.or.jp/report/wg2-2/e11-cn3.pdf

電子署名利用者システム構築・利用ガイドライン

http://www.ecom.jp/press/20010412_riyousya.html

http://www.ecom.or.jp/ecit/ecomjournal/no2/wg_an1_j02.htm

報告書本体

http://www.ecom.jp/report/h12seika/certification_wg/cert_wg1.pdf

各認証局のCP,CPS

日本認証サービス　AccreditedSign Certificate Policy and Certification Practice Statement (V1.51)

http://www2.jcsinc.co.jp/repository2/ASignCPS.pdf