第４節　その他の動向について

１　法務省

（１）商業登記法等の一部を改正する法律案

法務省は、平成１２年２月、インターネットを利用する電子商取引の増加に伴い、取引の安全性を担保するため商業登記情報を活用した電子認証制度を創設する商業登記法改正案と、公証人が電子文書で作成された委任状などを認証できるようにした電子公証制度を導入する公証人法改正案を国会に提出した。

商業登記法改正案では、登記所が会社の代表者の印鑑を証明する現行の印鑑証明制度に加え、会社の代表者が電磁的記録の作成者が電磁的記録の作成者を示す措置を講じたことを確認するために必要な事項を登記官が証明する制度を導入するものとしている。また、法務大臣の指定する登記所間においては、印鑑を提出した登記所以外の登記所に対しても、印鑑証明書の交付を請求することができるものとしている。

公証人法改正案では、公証人は、申請人が電磁的記録に一定の措置（当該電磁的記録の作成者を示すもの）を施したことを確認し、これを電磁的に認証することができるものとしている。また、公証人は、申請人の電磁的記録に、電磁的な確定日付を付すことができるものとしている。

２　自治省

（１）総合行政ネットワークの構築における行政情報の交換・提供方法の調査研究

自治省の外郭団体である（財）地方自治情報センターは、地方公共団体間の情報通信ネットワークをいかに構築し運営していくかの方策を提示するために、「総合行政ネットワーク構築に関する調査研究」を行い検討を進め、平成１１年３月、「総合行政ネットワークの構築における行政情報の交換・提供方法の調査研究」を公表した。

同報告書では、行政事務の効率化・迅速化に資するため地方公共団体間に構築する総合行政ネットワークを一定の共通仕様のもとに構築し、業務にとらわれることなく、柔軟で汎用的なものとするための考え方が示されている。

また、総合行政ネットワークにおいては、ネットワークシステムにおける機密性確保のために公開鍵基盤を使用した認証を行うべきとしている。認証単位としては団体認証、組織認証及び個人認証が考えられるが、総合行政ネットワークでは団体認証を採用すべしとしている。認証局については、システム資源を効率的に使えること、人的資源の確保が容易なこと及び運営なことを理由に、全地方公共団体の認証を１ヶ所に集中的に行うことを提言している。

（２）個人認証基盤に関する検討

現在、既に民間認証機関において個人認証サービスが提供されているが、特に厳格な認証を要する行政手続や取引等においては、住民たる個人を認証する根拠を持たない民間認証機関の個人認証サービスでは対応できない限界があるとしている。

そこで、住民基本台帳や印鑑登録証明によって個人に対する認証を行なっている地方公共団体による普遍的な個人認証基盤の構築が有望であり、このような個人認証基盤は、ネットワーク上で申請・届出等手続を行う電子申請のみならず、近年急速に発達しつつある電子商取引においても活用が期待され、将来、我が国全体の情報化の促進、住民の利便性の向上に大きく寄与すると予想されるとし、現在、その制度の在り方について検討を行なっている。

３　経団連「GBDe（Global Business Dialogue on Electronic Commerce）」

（１）GBDe パリ総会

GBDe は、日米欧の主要企業が参加している電子商取引の国際民間組織であ

り、１９９９年９月、パリにて会議を開催した。同会合では、「認証・セキュリティー」、「消費者信用」、「コンテンツ」、「情報基盤」、「利害関係者の責任」、「知的財産権」、「裁判管轄」、「個人データの保護」、「税・関税」のイシューに分かれ検討を行い、電子商取引の世界的なルール作りのために各国政府への具体的な提言をまとめた。今後、ＧＢＤｅは、各国政府が当該提言をどれだけ履行するか監視することとしている。

第５章　電子認証制度のセキュリティ確保方策

第１節　なりすまし犯罪防止対策の必要性

オープンネットワークの普及による情報流通の高速化・グローバル化、特にオープンネットワークを利用した電子商取引の本格的な発展・普及には各方面からの熱い視線が注がれており、大いなる期待の目で迎えられている。

しかしながら、他方で、ネットワーク社会は匿名性、無痕跡性、時間的・場所的無限定性、超高速性等をその特徴としており、本格的なネットワーク社会の到来により、犯罪者等が自ら身分を明かさず、犯罪等の証跡も残さずに、国際的な規模で一瞬にして利用するすべての者がこれらの犯罪者等の被害者になる可能性があり、実際、本年２月の官公庁に対するホームページ書換え事件、５月の「I love you」ウィルス事件のような世間を騒がした事件のほか、他人名義（架空人を含む。）の銀行口座、メール等を利用して行うなりすましによる詐欺等の犯罪が行われ、多くの国民が被害に遭っているところである。

しかも、ネットワーク社会の特徴に鑑みれば、事後の犯罪に対する取締りはもとより、事前の犯罪発生抑止対策という観点が極めて重要となる。このようなネットワークを利用した犯罪等を防止するために最も重要なことは、なりすましを防止するネットワークにおける「本人確認」と情報の漏洩、盗聴、改ざん等を防止する「情報の保護」の課題を解決することである。

そのためには、認証機能（「本人確認」の機能）及び秘匿機能（「情報の保護」の機能）を有する暗号技術を利用することが極めて有効であり、現に電子商取引等においても利用され始めているところである。このように、暗号技術は、適正に利用される限り、電子商取引の健全な発展や犯罪の防止に必要なものであることから、その普及を図るための施策を講じていく必要がある。

しかしながら、その一方で、暗号技術は、誰もが自由に利用することができることから、犯罪に係る電磁的記録の暗号化による隠蔽、暗号技術を利用することによりネットワーク上の身分証明を行う認証機関を悪用したなりすまし等の不正行為に利用されるおそれもあり、電子認証制度の信頼性が大きく損なわれ、電子商取引の発展をも阻害する可能性もある。

以上のようなことから、暗号技術の普及を図る場合には、同時にこのような暗号技術の不正利用対策も講じていく必要があり、公開鍵登録時の十分な本人確認の実施、認証機関の人的・物的適格性等犯罪防止の観点を踏まえた電子認証制度の構築を行っていく必要がある。

第２節　結語

この度成立した「電子署名及び認証業務に関する法律」では、認定認証機関に係る業務に関し、その利用者についての重大な被害が生じることを防止するため必要があると認められるときは、国家公安委員会は主務大臣に対し必要な措置をとるべきことを要請でき、また、認定認証事業者に対し、その認定に係る認証業務に関し、虚偽の申込みをして、利用者に不実の証明をさせた者に対し罰則を課す規定が盛り込まれており、ある程度犯罪防止の観点を踏まえた電子認証制度が構築されたと評価することができる。

しかしながら、このような規定の対象となるのは認定認証機関だけであり、無認定の認証機関は対象でない上、これらの認証機関は認定認証機関が満たさなければならない基準に適合する必要もない。しかも、基準自体が共同省令においてどの程度厳格なものとなるかも明確ではない。したがって、ユーザーが安全性の低い認証機関を悪用し、他人になりすまして行われる犯罪等が発生する可能性は残る。

したがって、今後、ユーザーに対し、より安全性の高い認証機関を利用するよう広報・啓発に努めるとともに、無認定の認証機関について、認定認証機関が満たすべき要件の充足性

の確保を求めるとともに、認定基準についても法第３７条を活用し、より安全性の高いものとなるとなるよう努めていくことが重要である。その際には、民間における認証機関に対する多種多様なニーズへも配慮し、両者の適切な関係を踏まえた制度的枠組みの在り方について、行政の関与の在り方も含めた再検討を今後継続的に行っていくことが必要である。