＜印国＞

情報技術の保護

H K ACHARYA & COMPANY, Ahmedabad
Dr. Rajeshkumar Acharya &
Girishchandra Tanna

インドは、電子商取引と電子行政を推進すべく、「2000 年情報技術法」を制定した。この法律は 2000 年 10 月 17 日より施行されている。

この法律は電子的記録とデジタル署名に法的効力を与えている。これによって、電子媒体を通じた契約の締結、権利・義務の発生が可能になっている。

この法律は、デジタル証明書を発行する認証局を監督する制度的枠組みを整えている。取引その他の悪用を防止するため、この法律に違反した場合の民事上・刑事上の責任を定めている。

この法律は、政府諸機関における電子的記録とデジタル署名の使用と承認について定めている。

この法律は、外国の認証局の効力について定めている。認証局は、電子証明を発行するには、認証局の管理官からのライセンスを付与されなければならない。

この法律の特徴を箇条書きにすれば、以下のようになる。

・デジタル署名は、電子的記録の認証の唯一の手段として認定される。
・電子的記録の認証は、非対称的暗号システムとハッシュ関数によってなされなければならず、それによって最初の電子的記録は別の電子的記録に暗号化・変換されなければならない。
・署名者の公開鍵を使う者は誰でも電子的記録を認証できる。
・秘密鍵と公開鍵は、署名者ごとに異なり、鍵ペアとして機能する。
・署名者とは、電子証明が発行された名前を持つ人物と定義される。
・公開鍵とは、デジタル署名を認証するために用いられる鍵ペアのうちの一つであり、デジタル証明書に挙げられているものと定義される。

・秘密鍵とは、デジタル署名を作るために用いられる鍵ペアのうちの一つと定義される。
・鍵ペアとは、秘密鍵と、それに数学的に関連している公開鍵を意味し、秘密鍵が作り出すデジタル署名を公開鍵が認証できるよう関連づけられているものと定義される。
・電子的記録とは、電子的な形式またはマイクロフィルムまたはコンピュータによって生成されたマイクロフィッシュで送受信される、データや、生成された記録またはデータ、蓄積された画像または音と定義される。
・データとは、定式化された方法で準備されているか、または準備されており、コンピュータ・システムまたはネットワーク内で処理される予定か、処理されているか、または処理されており、何らかの形式（コンピュータによる印刷物・電磁的または光学的保存媒体・パンチカード・パンチテープなど）になっているか、またはコンピュータのメモリ内に保存されている、情報・知識・事実・概念または指示と定義される。
・電子的記録は、電子的形式で利用可能な状態になっているか、そのように作られており、参照できるようになっていれば、法的な目的に用いられると認められる。
・電子的記録と電子署名の使用は、政府諸機関で認められる。
・電子的記録はその生成者に帰属する。
・電子的記録と電子署名のセキュリティを定める。
・管理官は認証局の監督の任に着く。
・誰でも認証局に電子証明の発行を申請することができる。
・認可されていない電子的記録の悪用や不正については、民事上・刑事上の責任を定める。

（邦訳：当研究所）

＜ India ＞

Protection of Information Technology

H K ACHARYA & COMPANY, Ahmedabad
Dr. Rajeshkumar Acharya & Girishchandra Tanna

India had enacted 'The Information Technology Act, 2000', to facilitate e-commerce and Electronic Governance. The Act is in force since October 17, 2000.

The Act provides for the legal recognition of electronic records and digital signatures. This enables the conclusion of contracts and the creation of rights and obligations through the electronic medium.

It provides for a regulatory regime to supervise the Certifying Authorities issuing Digital Signature Certificates. It provides for the civil and criminal liabilities for contravention of the Act to prevent misuse of transactions and other dealings.

The Act provides for the use and acceptance of electronic records and the digital signatures in the Government offices and its agencies.

It provides for the recognition of foreign Certifying Authorities. The Certifying Authority are granted license by the Controller of Certifying Authorities to issue electronic signature certificates.

Salient features of the Act are as under :

• Digital signature, is recognized as the sole method of authentication of electronic records

• Authentication of the electronic record should be effected by the use of asymmetric crypto system and hash function, which envelop and transform the initial electronic record into another electronic record

• Any person by use of a public key of the subscriber can verify the electronic record

• The private key and the public key are unique to the subscriber and constitute a functioning key pair
• Subscriber is defined to mean a person in whose name the Electronic Signature Certificate is issued
• Public key is defined to mean the key of a key pair used to verify a digital signature and listed in the Digital Signature Certificate
• Private key is defined to mean the key of a key pair used to create a digital signature
• Key pair is defined to mean a private key and its mathematically related public key, which are so related that the public key can verify a digital signature created by the private key
• Electronic record is defined to mean data, record or data generated, image or sound stored, received or sent in an electronic form or micro film or computer generated micro fiche
• Data is defined to mean a representation of information, knowledge, facts, concepts or instructions which are being prepared or have been prepared in a formalized manner, and is intended to be processed, is being processed or has been processed in a computer system or computer network, and may be in any form (including computer printouts, magnetic or optical storage media, punched cards, punched tapes) or stored internally in the memory of the computer
• Electronic records have been recognized for legal purpose, if it is rendered or made available in an electronic form and accessible for a subsequent reference
• Use of electronic record and electronic signature allowed in Government and its agencies
• Electronic records are attributed to the originator
• Security of electronic record and electronic signature provided
• The Controller is entrusted supervision over the Certifying Authorities
• Any person can make application to the Certifying Authority to issue Electronic Signature Certificate
• Civil and criminal liabilities provided in cases of unauthorized and/or misuse, fraud/ cheating of electronic records