New Regulations for E-Commerce in Japan

Masao Yanaga

In order to catch up with the development in computer and telecommunication technology, Japan has introduced or amended several statutes concerning electronic commerce and computer law.[1]

First, the Basic Act on the Formation of an Advanced Information and Telecommunications Network Society[2] was adopted in order to promote the measures to realize an advanced information and telecommunications network society expeditiously and intensively. The Act provides the basic ideas and the basic policy for formulating measures, clarifying the responsibilities of the national and local governments. In accordance with this Act, the Strategic Headquarters for Promoting an Advanced Information and Telecommunications Network Society (*Kôdo Jôhô Tsûshin Nettowâku Shakai Suishin Senryaku Honbu*) was established in the Cabinet.

Second, the Electronic Signature and Electronic Certification Service Act[3] now provides a legal effect to certain electronic signatures and an accreditation scheme for private electronic certification service providers.

Third, the Commercial Registration Act[4] was amended in order to make it possible for the commercial registries to provide electronic certification services based on the commercial registration system.

---

1 It should be noted that the reports of the Study Group on the Legal System of Electronic Commerce, a study group sponsored by the Director of the Civil Affairs Bureau, Ministry of Justice, have much influence on such legislation. See the report of the system subcommittee <*http://www.moj.go.jp/ENGLISH/CIAB/ciab-18.html*> (in English) and the substantive law subcommittee <*http://www.moj.go.jp/PRESS/000300-1.html*> (in Japanese).

2 *Kôdo jôhô tsûshin nettowâku shakai keisei kihon-hô*, Law No. 144/2000.

3 *Denshi shomei oyobi ninshô gyômu ni kansuru hôritsu*, Law No. 102 /2000.

4 *Shôgyô tôki-hô*, Law No. 125/1963, last amended by Law No. 80/2001.

Fourth, the Notary Act[5] was amended in 2000 so that a designated notary may electronically attach an officially stamped date to a document to certify the existence of the document at a specific moment, or notarize an electronic private document to certify the authenticity of the document.

Fifth, with respect to private law aspects, two statutes are very important: the law regarding the exceptions to the Civil Code with respect to mistakes in consumer contracts and notices of acceptance in electronic commerce,[6] and the law amending certain statutes requiring the delivery of a writing.[7]

Sixth, the Unfair Competition Act[8] was amended in 2001 and regulates unfair use of domain names identical or similar to others' trademarks and so on.

---

5 *Kôshônin-hô*, Law No. 53/1908, last amended by Law No. 305/2000.

6 *Denshi shôhinsha keiyaku oyobi denshi shôdaku tsûchi ni kansuru minpo no tokurei ni kansuru hôritsu*, Law No. 95/2001. A brief introduction to the bill can be found in M. YANAGA, A Bill Regarding the Electronic Declaration of Intention in Japan: ZJapanR No. 11 (2001) 255-258.
Article 3 was modified in the course of the discussion at the Diet in order to protect consumers more clearly. The final wording of Article 3 of the law is as follows (the proviso to paragraph 1 was deleted and paragraph 2 was inserted; the modified wording is italicized):
Art. 3 (Exceptions to the Civil Code in respect to electronic consumer contract)
1. The proviso to Article 95 of the Civil Code shall not apply to cases of errors in the elements of an electronic consumer contract with respect to a consumer's declaration of intent to offer or accept the contract, if the error is a type listed below.
(1) Where the consumer was not willing to declare his intent to offer or accept an electronic consumer contract with the entrepreneur *as the other party to the electronic consumer contract (including his mandatory; hereinafter the same)* when he transmitted a message by the computer used by him;
(2) Where the consumer was willing to declare his intent for something different than an offer or acceptance of the electronic consumer contract when he transmitted a message by the computer used by him.
2. The preceding paragraph shall not apply where the entrepreneur, as the other party to the electronic consumer contract, has taken the following measures on the screen by electro-magnetic means when the consumer has declared his intent to offer or accept the electronic consumer contract:
(1) to request a consumer, where the consumer is willing to declare his intent to offer or accept a specified electronic consumer contract, to express his intent;
(2) to display clearly the content of the declaration of intent regarding the expression mentioned at the preceding item;
(3) to request the consumer to edit the content of the declaration of intent mentioned at the preceding item, if necessary, and confirm there are no errors;
(4) to request the consumer, where the consumer has confirmed in accordance with the preceding paragraph, to declare that he has confirmed;
(5) to request clearly the consumer to choose whether he will declare the intent the same as the declaration mentioned at the preceding item.

7 *Shomen no kôfu-tô ni kansuru jôhô tsûshin no gijutsu no riyô no tame no kankei hôritsu no seibi ni kansuru hôritsu,* Law No. 126/2000.

8 *Shiteki dokusen no kinshi oyobi kôsei torihiki no kakuho ni kansuru hôritsu*, Law No. 54/1947, last amended by Law No. 80/2001.

Last, the Unauthorized Computer Access Act[9] was introduced in order to counter increasing unauthorized computer access.[10]

I. Basic Act on the Formation of an Advanced Information and Telecommunications Network Society

Article 10 of the Basic Act on the Formation of an Advanced Information and Telecommunications Network Society provides that the national government has the responsibility to formulate and implement measures to establish an advanced information and telecommunications network society in accordance with the basic ideas provided in Articles 3 through 9. The basic ideas are as follows:

(1) realizing a society in which the people can enjoy the benefits of information and telecommunications technology (Art. 3);
(2) promoting the economic structural reform and enhancing the international competitiveness of industry (Art. 4);
(3) realizing citizen life that evokes feelings of comfort and affluence (Art. 5);
(4) realizing vital local communities and improvement of the welfare of residents (Art. 6);
(5) role sharing between the national/local governments and the private sector (Art. 7);
(6) filling gaps in the opportunities for access to information and telecommunications technology (Art. 8); and
(7) dealing with new problems that emerge in line with changes in the socioeconomic structure (Art. 9).

Local governments have the responsibility to formulate and implement measures of their own that reflect distinctive features of the territories of the relevant local governments with regard to the formation of an advanced information and telecommunications network society, while appropriately sharing this role with the national government (Art. 11). The national and local governments mutually cooperate so that measures for an advanced information and telecommunications network society will be implemented expeditiously and intensively (Art. 12). The government will take legal, fiscal, and other actions necessary for implementing measures to establish an advanced information and telecommunications network society (Art. 13).

According to Article 25 of this Act, the Strategic Headquarters for Promoting an Advanced Information and Telecommunications Network Society (hereinafter referred to as the "Headquarters") was established in the Cabinet. The Headquarters is responsible for making a priority policy program for the formation of an advanced information and

9 *Fusei akusesu kôi no kinshi-tô ni kansuru hôritsu*, Law No. 128/1999, last amended by Law No. 160/1999.

10 The Electronic Signatures and Electronic Certification Service Act has some penal provisions concerning an application for untrue electronic certification and an illegal use of the mark of an accredited certification service provider.

telecommunications network society (hereinafter referred to as the "priority policy program"). At the same time, it is a mission of the Headquarters to plan important measures to establish an advanced information and telecommunications network society, and to implement such measures (Art. 26). The priority policy program should have provisions with respect to:

(1) the basic policy concerning measures that the government should implement expeditiously and intensively in order to establish an advanced information and telecommunications network society;
(2) the measures that the government should implement expeditiously and intensively in order to drive the Japanese society forward to the most advanced information and telecommunications society in the world;
(3) the measures that the government should implement expeditiously and intensively in order to promote education/learning as well as to develop human resources with respect to information and telecommunication technology;
(4) the measures that the government should implement expeditiously and intensively to facilitate e-commerce, etc.;
(5) the measures that the government should implement expeditiously and intensively to make administrative procedures digitized, applying information and telecommunications technology to the public sector;
(6) the measures that the government should implement expeditiously and intensively to ensure the security and reliability of advanced information and telecommunications networks; and
(7) other measures that are required for the government to drive forward expeditiously and intensively in order to realize an advanced information and telecommunications network society (Art. 35 para. 2).

The Headquarters consists of all state ministers and those who have superior insights into the formulation of an advanced information and telecommunications network society and have been appointed by the prime minister (Art. 30).

II. ELECTRONIC SIGNATURE

The Electronic Signatures and Electronic Certification Service Act provides the legal effect of an electronic signature to some extent. An electro-magnetic record that is prepared in order to provide information – except for that produced by a public official in the course of his official functions – is presumed to be authentic if an electronic signature is made by the named person in relation to the information recorded in an electromagnetic record,[11] provided that such an electronic signature is made under the proper

11 Since there are no explicit provisions regarding admissibility of evidence in civil procedures and freedom of proof is the general rule, the courts have admitted electro-magnetic records. In addition, the courts have a discretionary power to a reasonable extent regarding the evi-

control of the codes and objects necessary to produce the signature under the exclusive control of the signatory (Art. 3).

For the purpose of this Act, an "electronic signature" is defined as a measure taken with regard to information that can be recorded in an electro-magnetic record.[12] At the same time, an electronic signature should be a measure to indicate that the person who has taken the measures created the information, and to confirm whether or not the information has been altered (Art. 2 para. 1).

III. Private Electronic Certification Service

Though there is no restriction on providing electronic certification services in Japan,[13] the Electronic Signatures and Electronic Certification Service Act provides an accreditation scheme for electronic certification providers. A person seeking to perform or who has been performing designated certification service may be granted an accreditation from the competent ministers (Art. 4 para. 1).

For the purpose of this Act, "certification service" is defined as a service that, in response to either the request of the user[14] or the request of another person, certifies that a device used to confirm that the user performed an electronic signature belongs to the user (Art. 2 para. 2). "Designated certification service" is defined as a service certifying an electronic signature which can be made solely by the registrant and satisfies the standards provided in the ordinances of the competent ministries according to the method used for the electronic signature (Art. 2 para. 3).[15]

A person seeking to receive such an accreditation should, in accordance with the provisions in the ordinances of the competent ministries, file with the related ministers

---

dential value of the evidence (Art. 247 Civil Procedure Act [*Minji soshô-hô*] Law No. 109/1996, last amended by Law No. 96/2001).

12 Any record that is produced by electronic, magnetic, or any other means unrecognizable by natural perceptive function, and is used for data processing by a computer.

13 There is no restriction on use of cryptography in Japan.

14 A "user" is a person who makes use of such service with regard to the electronic signature that he himself makes.

15 Article 2 of the Enforcement Regulation for the Electronic Signature and Electronic Certification Service Act (Ministry of Public Management, Home Affairs, Post and Telecommunication, Ministry of Justice and Ministry of Economics, Trade and Industry Ordinance No. 2 of 2001) provides the standard. The security of an electronic signature must be based on the difficulty of one of the following computation:
(1) factoring an integer that is the product of two distinct odd primes and not less than 1024 bits long;
(2) finding discrete logs in the multiplicative group in a finite field not less than 1024 bits;
(3) finding discrete logs in a group on an elliptic curve not less than 160 bits;
(4) another computation that the competent ministers deem to be as difficult as the preceding three computation methods.

an application form that states the following particulars, as well as other documents prescribed by the ordinances of the competent ministries:

(1) the name and address, and, for an organization, the name of its representative; and
(2) an outline of the facilities used for the service and the method of providing the service (Art. 4 para. 2).

When the competent ministers have granted an accreditation, they should make a public announcement of that fact (Art. 4 para. 3).

Article 5 of the Act stipulates that an accreditation may not be granted to:

(1) a person who has been sentenced to a penalty of imprisonment or more serious penalty (including an equivalent penalty pursuant to the laws and regulations in a foreign country), or who has been sentenced to such a penalty pursuant to this law unless two years have passed since the day on which either the enforcement of said penalty finished or the person came to be no longer subject thereto; or
(2) a person whose accreditation has been revoked pursuant to the provisions of either paragraph 1 of Article 14 or paragraph 1 of Article 16 unless two years have passed since the day of the revocation; or
(3) an organization whose director performing the service falls within (1) or (2).

The competent ministers should grant an accreditation only when they find that the application for accreditation conforms to all of the following requirements:

(1) the facilities, including hardware and software, used for the service applied for accreditation fulfill the requirements prescribed in the ordinances of the competent ministries;[16] and
(2) the confirmation in the service applied for accreditation of the identity of the user is performed through a method prescribed in the ordinances of the competent ministries; and the service applied for accreditation is performed through a method that conforms to the requirements prescribed in the ordinances of the competent ministries[17] (Art. 6 para. 1).

---

16 Article 4 of the Enforcement Regulation for the Electronic Signature and Electronic Certification Service Act provides the requirements as follows:
(1) The facilities used for offering the certification service should be installed in the place under the admission control;
(2) Necessary measures should be taken to prevent illegal access via telecommunication line to the facilities used for offering the certification service;
(3) Necessary measures should be taken to protect the facilities used for offering the certification service against illegitimate persons and to log the operation of such facilities;
(4) The computer used as the certification provider's signature creation device should be for the exclusive use of signature devices and have the necessary functions to keep the secrecy of the private keys;
(5) Necessary measures should be taken so that the facilities used for offering the certification service and the admission control devices should not be damaged in cases of power failures, earthquakes, fires, floods, and other disasters.

17 An accredited electronic certification service provider should require a prospective user to show his passport; the license, permit, or qualification certificates issued by the authorities;

In the course of the review necessary for the accreditation, the competent ministers should, in accordance with the provisions in the ordinances of the competent ministries, perform on-site investigation of the system involved in the implementation of the service applied for accreditation (Art. 6 para. 2). However, the competent ministers may designate an investigating organization to conduct the whole or part of the investigation provided in Article 6, paragraph 2 (Art. 17 para. 1). Such designation shall, in accordance with the provisions in the ordinances of the competent ministries,[18] be made upon the application of the person seeking to conduct the investigation (except for a person seeking to conduct such an investigation at an office located in a foreign country) (Art. 18).

Where the competent ministers have designated an investigating organization, they cannot conduct by themselves the whole or part of the investigation. In this case, the competent ministers should, taking the results of the investigation done by the designated investigating organization into account, grant an accreditation or a renewal of such an accreditation (Art. 17 para. 2).

When the designated investigating organization has conducted such an investigation, it shall, in accordance with the provisions in the ordinances of the competent ministries, give notice of the results of the investigation to the competent ministers without delay (Art. 17 para. 4).

The accredited certification service provider shall instruct the applicant of material information concerning implementation of electronic signatures and use of the certification service (Enforcement Regulation for the Electronic Signature and Electronic Certification Service Act[19], Art. 6 no. 1). Insofar as the accredited certification service provider provides signature keys, he shall deliver the private key in a safe and trustworthy way and delete the private key and its copy (Enforcement Regulation for the Electronic Signature and Electronic Certification Service Act, Art. 6 no. 3). The validity period of a certificate may not be longer than five years (Enforcement Regulation for the Electronic Signature and Electronic Certification Service Act, Art. 6 no. 4). A certificate

---

his foreigner's registration certificate and identification card (with photos) issued by a public authority; and the certificate of his seal registration, etc. At the same time, he must submit a copy of his resident's card and a copy or an abstract of his family register or a certificate of the particulars in the foreigner's register in order for the service provider to confirm the identity of the prospective user (Enforcement Regulation for the Electronic Signature and Electronic Certification Service Act, Art. 5).

18 Japan Quality Assurance Organization is designated as the designated investigating organization (Ministerial Ordinance designating the designated investigating organization in accordance with paragraph 1 of Article 17 of the Electronic Signature and Electronic Certification Service Act [*Denshi shomei oyobi ninshô gyômu ni kansuru hôritsu 17jô dai 1kô ni kitei suru chôsa kikan wo shitei suru shôrei,* Ministry of General Affairs, Ministry of Justice and Ministry of Economics, Trade and Industry Ordinance No. 3/2001]).

19 *Denshi shomei oyobi ninshô gyômu ni kansuru hôritsu shikô kisoku*, Ministry of General Affairs, Ministry of Justice and Ministry of Economics, Trade and Industry Ordninance No. 2/2001.

issued by an accredited electronic certification service provider shall bear the provider's electronic signature that meets the requirement in Article 2[20] of the Enforcement Regulation for the Electronic Signature and Electronic Certification Service Act (Enforcement Regulation for the Electronic Signature and Electronic Certification Service Act, Art. 6 no. 6), and shall contain the following information:

(1) the name of the issuer (that is, certification service provider) of the certificate and the serial number of the certificate;
(2) the date of issuance, and the beginning and the end of the certificate's validity;
(3) the name of the user (that is, signature key owner);
(4) the designation of the algorithms for the signature testing key of the user and the signature testing key of the certification service provider.

IV. Electronic Certification Services based on the Commercial Registry

In addition to private electronic certification services providers, there is an official certification system based on the commercial registration system in Japan. The commercial registry has begun to play a role as an electronic certification service provider for companies.[21]

In Japan, certain matters related to merchants, including companies, are registered in the commercial register. As for companies, such important particulars such as the purpose, the name, the principal office, branches, and directors must be registered (Commercial Code[22], Art. 188; Limited Liability Companies [GmbH] Act[23], Art. 13). The public may access the register (Commercial Registration Act, Art. 10) and request certified copies of the commercial register (Commercial Registration Act, Art. 11).

Under this system, an impression of a seal (*inkan*) of an applicant for registration is submitted in advance to the commercial registry to identify the applicant for registration (Commercial Registration Act, Art. 20). And the commercial registry issues a certificate of an impression of a seal to one who submits a seal to the commercial registry (Commercial Registration Act, Art. 12). For a long time, a corporation's certified copy of the commercial register, a certificate of qualifications, and a certificate of an impression of a seal (all of which are based on the information registered in the commercial register) have been widely used as a means to confirm the other party and his power of representation. Accordingly, it is inexpensive and natural to establish an electronic certification system based on the commercial registration system. Japanese people have trust in the commercial registration system as a legal system ensuring the reliability of operations of the commercial registry with skills in registration and publication of informa-

20 *Supra* note 15.
21 This service already became available in Tokyo and major cities in 2000.
22 *Shôhô*, Law No. 48/1899, last amended by Law No. 79/2001.
23 *Yûgen kaisha-hô*, Law No. 74/1938, last amended by Law No. 79/2001.

tion. Thus, an electronic certificate issued by the commercial register will be treated as reliable as a corporation's exemplified copy of the commercial register, a certificate of qualification, and a certificate of an impression of a seal.

Upon request, the commercial registry issues an electronic certificate on the public key of the electronic signature of an applicant (Commercial Registration Act, Art. 12*bis*). The commercial registry uses asymmetric cryptography. Details are prescribed in an ordinance of the Ministry of Justice.[24] The validity period of a certificate is decided in accordance with the applicant's request, but it may not be longer than two years and three months (Commercial Registration Regulation,[25] Art. 33*bis*).

V. ELECTRONIC NOTARY

In Japan, the Notary Act governs the notarization system and the notaries[26] provide the notary service. Notaries can attach an officially stamped date to certain documents to certify the date when a document is prepared (Enforcement Act for the Civil Code[27], Art. 5 para. 2 and Art. 6). To prevent future disputes, they can examine the contents of certain documents to notarize private documents and certify the existence and the contents of those documents (Notary Act, Art. 1). In addition, notaries can prepare notarial documents to certify the execution of contracts and the legitimacy of their contents.

Under the amended Notary Act (Art. 1 no. 4), a designated notary[28] shall attach an electronic officially stamped date and his/her electronic signature to an electronic document (electronic official date stamping). A designated notary shall also notarize an electronic private document. This notary shall inspect the contents and effectiveness of an electronic private document and attach a certification statement and his/her electronic signature to the document (Notarization of an Electronic Private Document). In addition, such a notary should store, in accordance with the provisions in an ordinance of

---

24 Commercial registries shall use the method provided in Appendix D to the Japanese Industrial Standards X5731-8 (RSA algorithm). The key should be 1024 bits or 2048 bits long (Commercial Registration Regulation, Art. 33quarter).

25 *Shôgyô tôki kisoku*, Ministry of Justice Ordinance No. 23/1964, last amended by Ordinance No. 65/2001.

26 The Minister of Justice appoints and supervises notaries who have professional knowledge and careers in legal affairs. Notaries should act in a disinterested and public position (in relation to this, there are restrictions on notaries holding other jobs [Notary Act, Art. 5]). The Penal Code (*Keihô*, Law No. 45/1907, last amended by Law No. 97/2001, Art. 156) and other statutes ensure the disinterested operation of notaries. Finally, the State Redress Law (*Kokka baishô-hô,* Law No. 125/1947) would be applied to inappropriate operations of notaries.

27 *Minpô shikô-hô,* Law No. 11/1898, last amended by Law No. 40/2000.

28 Only the notaries designated for electronic public notary services by the Ministry of Justice will offer such services (Notary Act, Art. 7bis).

the Ministry of Justice,[29] the information necessary for verifying the identity of the information recorded in the notarized electro-magnetic document. Upon request of the applicant, the notary shall store electro-magnetic notarized documents and electronic officially stamped documents and certify the existence and the contents of the electronic documents (Commercial Registration Act, Art. 62*septies*).

VI. Law Amending Certain Statutes Requiring the Delivery of Writing

Under the Civil Code,[30] a contract can be formed, in principle, either verbally or in writing. Though there have been no general formality requirements for contracts in Japan, there have been several statutes requiring a "writing (*shomen*)", mainly for protecting consumers, investors, or a party who has less bargaining power than the other party.[31] Such statutes provide the particulars to be shown in a writing but do not give the definition of "writing", and it has not always been clear that electronic contracts meet a "writing" requirement. Some believe that an electronic contract usually satisfies the "writing" requirement because an electronic contract is visible on a computer screen and the data of the contract may be stored in a hard disk or other memories. Others consider that it cannot satisfy such a requirement because a "writing" should have some element of permanence that can be called upon at a future time. It has been suggested that the writing requirements have been an impediment to the development of e-commerce and, at the same time, an electronic document is enough for the purpose in many cases. Thus, the law amending certain statutes requiring the delivery of writing has amended 50 statutes[32] in order to allow businesses to deliver an electronic document instead of paper-based document (writing), provided that the customer or member has agreed to be delivered documents in electro-magnetic form. In other words, these amendments allow the use of electronic documents in cases where both the producer and the recipient of the documentation have agreed to do so. The Ministry of Economics, Trade, and Industry has interpreted that the amendments allow the parties to use

---

29 Designated notaries shall attach their electronic signature using RSA algorithm (Appendix D to the Japanese Industrial Standards X5731-8) with a 1024-bit-long or 2048-bit-long key (Ministerial ordinance on the services of the designated notaries on electro-magnetic records [*Shitei kôshônin no okonau denji-teki kiroku ni kansuru jimu ni kansuru shôrei,* Ministry of Justice Ordinance No. 24/2001], Art. 2).

30 *Minpô*, Law No. 89/1896 and Law No. 9/1898, last amended by Law No. 41/2001.

31 For example, the Act Regarding Door-to-Door Sales and Other Direct Sales, the Travel Agency Act, and the Securities Exchange Act require a "writing" to protect consumers or customers.

32 Including the Travel Agency Act, the Act Regarding Door-to-Door Sales and Other Direct Sales, the Securities and Exchange Act, the Financial Futures Transaction Act, the Asset Securitization Act, the Investment Trust and Investment Corporation Act, the Securities Investment Advisor Act, the Commodity Investment Business Act, the Installment Sales Act, and the Real Property Dealing Business Act.

e-mail, facsimiles, and web sites[33] as well as the physical delivery of CD-ROMs or floppy disks.

VII. Unfair Competition Act and Domain Names

In order to prevent cybersquatting, the 2001 amended[34] Unfair Competition Act provides that "unfair competition" covers registering, possessing, or using a domain name which is identical or similar to the indication of other's goods, etc. – names, trade names, trademarks, marks, and those indicating goods or services and relating to other's business – with a bad-faith intent to profit or an intent to harm others (Unfair Competition Act, Art. 2 para. 1 no. 12).

One who has been or is likely to be damaged in their business interests by unfair competition may require the other who is infringing or is likely to infringe upon the interests to discontinue or refrain from such infringement (Unfair Competition Act, Art. 3 para. 1). Such a claimant who is acting in accordance with the provisions of paragraph 1 of Article 3 may demand the destruction of the articles by which the infringement was committed, the disposal of the articles used for the infringement, or other measures necessary to prevent the infringement (Unfair Competition Act, Art. 3 para. 2). A person who has infringed intentionally or negligently on others' business interests shall be liable for the damages caused from his unfair competition. In such a case, the profits, if any, obtained by the infringing person from that infringement are presumed to be the amount of damages suffered by the victim (Unfair Competition Act, Art. 4 para. 1). The victim may choose to claim the amount equivalent to the amount that would have been received by them through a usual exercise of the right of such a domain name (Unfair Competition Act, Art. 4 para. 2 no. 4). However, the provisions of paragraph 2 of Article 4 do not prejudice any claim for damages in excess of the amount mentioned therein. In such a case, the court may consider the absence of any bad faith and gross negligence on the part of the infringing person in fixing the amount of damages (Unfair Competition Act, Art. 4 para. 3). In addition, the victim may require

---

33 The "i-mode", which is very popular among young people in Japan, may also be included if the demand exists. The "i-mode" is an information system using cellular telephones with a picture-transmitting function.

34 In Jaccs v. Nihonkai Pact (Toyama District Court, Decision of 6 December 2000, affirmed Kanazawa Branch of Nagoya High Court, Decision of 10 September 2001)
These decisions can be found on the homepage of the Supreme Court under <*http://courtdomino2.courts.go.jp/chizai.nsf/*>. The court held that the plaintiff is entitled to an injunction against the defendant's commercial use in commerce under the Unfair Competition Act (before the amendments of 2001). In this case, the plaintiff's trade name was famous at the time of registration of the domain name, and the defendant's domain name is identical or confusingly similar. At the same time, the court recognized that the defendant has registered and been using the domain name with a bad-faith intent to profit from that name.

the person who has damaged the reputation of the other's business intentionally or negligently to take measures necessary to recover the victim's reputation, either instead of compensating damages or together with compensation of damages (Unfair Competition Act, Art. 7).

VIII. Unauthorized Computer Access Act

The Unauthorized Computer Access Act prohibits unauthorized computer access (Art. 3). This Act also stipulates the measures to be taken by the Metropolitan or Prefectural Public Safety Commissions for preventing a recurrence of such acts, in order to prevent computer-related crimes that are committed through telecommunication lines and to maintain the telecommunications-related order that is realized by access control functions.

1. Unauthorized Computer Access

A person who has committed an unauthorized computer access shall be punished with imprisonment with labor not longer than one year or a fine of not more than 500,000 yen (Art. 8). Under this Act, unauthorized computer access is defined as follows (Art. 3 para. 2):

(1) making available a specified use which is restricted by an access control function, inputting, via telecommunication line, another person's identification code for the access control function into the specified computer that has an access control function (excluding such acts done by the access administrator who has implemented the said access control function, or conducted with the approval of the access administrator or of the authorized user for that identification code);
(2) making available a restricted specified use of a specified computer that has an access control function, inputting, via telecommunication line, any information (excluding an identification code) or command that can evade the restrictions placed by that access control function on that specified use to the specified computer (excluding such acts done by the access administrator who has added the access control function concerned, or conducted with the approval of the access administrator);
(3) making available a restricted specified use of a specified computer, which is restricted by an access control function installed into another specified computer which is connected, via a telecommunication line, to that specified computer, inputting, via a telecommunication line, any information or command that can evade the restrictions into the other computer.

An "identification code" is defined as a code granted to a person (hereinafter referred to as "authorized user") who has been authorized by the access administrator, who administrates a specified use of a specified computer, with respect to the specified use

(hereinafter "authorized user and access administrator" are referred to as "authorized user, etc.") so that the access administrator can identify the authorized user, etc., distinguishing the latter from another authorized user, etc. An "identification code" should be one of the items (1) through (3) as follows, or a combination of these:

(1) a code whose content the access administrator is required not to make wantonly known to a third party; or
(2) a code that is compiled in such ways as are defined by the access administrator using an image of the body, in whole or in part, of the authorized user, etc., concerned, or his or her voice; or
(3) a code that is compiled in such ways as are defined by the access administrator using the signature of the authorized user, etc. (Art. 2 para. 2).

An "access control function" refers to a function governing a specified use that is added by the access administrator to a specified computer or to another specified computer that is connected to that specified computer through a telecommunication line in order to automatically control the specified use concerned with that specified computer. It removes all or part of the restrictions on the specified use after confirming that a code inputted into a specified computer having that function by a person who is going to conduct that specified use is the identification code (to include a code which is a combination of a code compiled in such ways as are defined by the access administrator concerned using an identification code and part of that identification code [Art. 2 para. 3]).

2. Assist to Unauthorized Computer Access

A person who has assisted another's unauthorized computer access shall be punished with a fine of not more than 300,000 Yen (Art. 9). It is prohibited to provide another person's identification code relating to an access control function to a third person, indicating that it is the identification code for a specified use of a specified computer, or at the request of a person who has such knowledge. However, such acts are allowed in cases where they have been done by the access administrator, or with the approval of the access administrator or of the authorized user.

ZUSAMMENFASSUNG

Im Anschluß an den Beitrag des Verfassers in Heft 11 der ZJapanR gibt die vorliegende Untersuchung einen Überblick über die neuesten rechtlichen Entwicklungen im Bereich des elektronischen Geschäftsverkehrs in Japan. Verschiedene neue Gesetze sind in diesem Jahr in Kraft getreten; zahlreiche andere wurden ergänzt. Die Analyse beginnt mit dem „Grundlagengesetz zur Entwicklung einer Gesellschaft, die auf fortgeschrit-

tenen Informations- und Telekommunikationsnetzwerken beruht". Es schließt sich ein Überblick über die Regeln für elektronische Unterschriften und die in einem weiteren Sondergesetz festgelegten Vorschriften zur elektronischen Zertifikation an. In Ergänzung zu diesen Sondergesetzen sind die registerrechtlichen Vorschriften im Handelsgesetz wie im GmbH-Gesetz geändert worden, und zudem wurde das Handelsregistergesetz angepaßt. Zahlreiche Formvorschriften im Gesetz über die Zwangsvollstreckung, dem Notargesetz und dem Zivilgesetz sind ebenfalls mit Blick auf den elektronischen Geschäftsverkehr überarbeitet worden. Schließlich werden Fragen des unlauteren Wettbewerbs und ein neues Gesetz gegen einen unerlaubten Zugriff auf Datennetze vorgestellt.

(die Red.)