Recent Cybercrime Legislations in Japan

Takato Natsui

Professor at school of law and graduate school of law at Meiji University
Vice Chair and director at the Information Network Law Association Japan
Director at the Law and Computer Association Japan
Attorney at Law (Tokyo Bar Association)

Summary

The Internet has an increasingly importance all over the world. However many legal issues (for instance cybercrimes, digital copyright protection or personal data protection) also have been taken place. As the result cyber legislation is also one of the most important concerns among modern countries.

This article presents an overview of current cybercrime legislation in Japan, points out some problems involved in such legislation and suggests the importance to establish a uniform legislation policy for better legislation in future.

Keywords

Cybercrime, cyberlaw, information society, Internet, legislation, treaty

1. Introduction

Since 1995, the Internet has been continuously growing up. Currently the Internet would be one of the most important measures for our daily life. Numerous people have been using the Internet for the purpose of sending their emails, retrieving necessary information, publishing their articles, enjoying games, making friends, seeking new customer and binding business contracts.

However criminal people also have been able to be an Internet user, and there have been many illegal contents on the Internet as well as other cybercrimes. For instance hacking (unauthorized access), ID theft (credit card information theft or computer fraud), digital copyright infringement, cyber squatting (misuse of domain names), privacy intrusion, defamation on the Web, network fraud, SPAM (unsolicited bulk commercial email messages), misuse of law enforcement power (illegal interception of people's telecommunication) and other illegal electronic transactions have been a serious concern for many people.

Due to such big change of social environment, the Japanese National Diet has enacted many new laws and amended relevant existing laws relating to the Internet, and courts of Japan also have been battling with such new problems which have taken place on the Internet. But in fact there are some lacks of laws to address the information society. These are current problems which are taken place not only in Japan but also in every other country. All countries may share common problems in the same information society. Due to this, similar new laws are enacted and drafted also in other countries, and many international treaties relating to the Internet have been bound between Japan and other countries (for instance the European Council

Cybercrime Convention of 2001 (ETS no. 185), WIPO new Copyright Treaty of 1996). Party countries have to address any requirements and obligations involved in such international treaties. We ought to examine such cyberlaw and relevant treaties as a comparative study for better legislation in future.

Especially cybercrime has been one of the most important problems among any cyber legislations all over the world. For example the explanatory report of the Cybercrime Convention (ETS 185)[1] points out such importance clearly in its introduction.

Introduction (ETS185)

1. The revolution in information technologies has changed society fundamentally and will probably continue to do so in the foreseeable future. Many tasks have become easier to handle. Where originally only some specific sectors of society had rationalised their working procedures with the help of information technology, now hardly any sector of society has remained unaffected. Information technology has in one way or the other pervaded almost every aspect of human activities.
2. A conspicuous feature of information technology is the impact it has had and will have on the evolution of telecommunications technology. Classical telephony, involving the transmission of human voice, has been overtaken by the exchange of vast amounts of data, comprising voice, text, music and static and moving pictures. This exchange no longer occurs only between human beings, but also between human beings and computers, and between computers themselves. Circuit-switched connections have been replaced by packet-switched networks. It is no longer relevant whether a direct connection can be established; it suffices that data is entered into a network with a destination address or made available for

[1] The Japanese government signed this convention in 23rd of 2001, but this convention has not been accepted and ratified at the National Diet of Japan yet.

anyone who wants to access it.

3. The pervasive use of electronic mail and the accessing through the Internet of numerous web sites are examples of these developments. They have changed our society profoundly.

4. The ease of accessibility and searchability of information contained in computer systems, combined with the practically unlimited possibilities for its exchange and dissemination, regardless of geographical distances, has lead to an explosive growth in the amount of information available and the knowledge that can be drawn there from.

5. These developments have given rise to an unprecedented economic and social changes, but they also have a dark side: the emergence of new types of crime as well as the commission of traditional crimes by means of new technologies. Moreover, the consequences of criminal behaviour can be more far-reaching than before because they are not restricted by geographical limitations or national boundaries. The recent spread of detrimental computer viruses all over the world has provided proof of this reality. Technical measures to protect computer systems need to be implemented concomitantly with legal measures to prevent and deter criminal behaviour.

6. The new technologies challenge existing legal concepts. Information and communications flow more easily around the world. Borders are no longer boundaries to this flow. Criminals are increasingly located in places other than where their acts produce their effects. However, domestic laws are generally confined to a specific territory. Thus solutions to the problems posed must be addressed by international law, necessitating the adoption of adequate international legal instruments. The present Convention aims to meet this challenge, with due respect to human rights in the new Information Society.

Of course these issues have same importance in Japan also.

The main aim of this article is to present an overview of new legislations relating to cybercrime in Japan. And the second aim is to point out some problems involved in current laws.

2. Overview of Cybercrime Legislation in Japan

In Japan there are many laws relating to the Internet and information society, and many scholars believe that such law is a cyberlaw[2]. These include intellectual property protection, electronic commerce, telecommunication, provider liability, personal data protection, electronic evidence and criminal procedure. Also there are many criminal activities relating to computer systems and computer data, and many scholars believe that such activities are cybercrimes.

However such laws have been enacted as a kind of ad hoc legislation and by different manner each other. For instance some of them have been enacted as new laws but others have been made as amendment of existing laws. In fact there is no official uniform policy for cyberlaw legislation in Japan.

On the other hand some people may think of such legislation as a new type law but other people may think of such legislation in accordance with a traditional legal dogmatic which is often conservative. As the result, many conflicts have been took place both in interpretation and in law enforcement practices of such laws.

In this article, I present some overviews of legislation relating to cybercrime.

[2] There is no official definition of what is the "Cyberlaw" at all, but we can discover some definitions of cyberlaw in many related books and articles. For the purpose of this article, I define the Cyberlaw as a kind of law relating to the Internet and digital data.

2.1 Main Cybercrimes

Main cybercrimes shall be punished under the Penal Code of Japan (Law No.45 of 1907, amended 1987) and the Unauthorized Computer Access Law (Law No. 128 of 1999).
Many cybercrimes defined in the Cybercrime Convention (ETS 185) are involved in these laws.

a) Crimes in Penal Code of Japan

The penal Code of Japan enacted in 1907, of course there was no computer system and computer data at the time. So the Penal Code had been amended in 1987. Main purpose of this amendment was to ensure a modern computerized business works by prohibiting any computer crimes, especially for protection a safety electronic fund transfer transactions and an integrity of any computer programs and electronic data.
However, similar to other Japanese law, the Penal Code has a few definition clauses. Only one definition clause relating to computer crimes is following.

(Definitions)
Article 7-2
The term "electromagnetic record" used in this Code shall mean the record made by any electronic method, magnetic method or other methods unrecognizable with human perception and provided for the use of data processing in computer system.

This definition clause is a kind of product before the Internet age.

By this amendment, the Penal Code of Japan has some types of cybercrime articles. Following activities shall be punished by the Penal Code.

a-1) Illegal production of electromagnetic record

Article 161-2 of the Penal Code prohibits any illegal production of electromagnetic record.

(Illegal production and use of electromagnetic record)
Article 161-2
Any person who with the intention of misleading any business management of others, illegally produces such electromagnetic record relating to legal right, duty of certification of a fact as to be provided for the use of the business management shall be punished with penal servitude for not more than five years or a fine for of not more than five hundred thousand yen.
2. The crime under the preceding paragraph involved in the electromagnetic record to be made by public offices officers shall be punished with penal servitude for not more than ten years or a fine for of not more than one million yen.
3. Any person who with the intention of paragraph 1, provides such electromagnetic record which is produced illegally and relating to legal right, duty of certification of a fact as to be provided for the use of the business management shall be punished with the same penalty as person who illegally makes the electromagnetic record.
4. Any person who attempts to commit any crimes set forth in preceding paragraph shall be punishable.

This Article is same to the computer-related forgery in the Cybercrime Convention Article 7.

Article 7 Computer-related forgery (ETS 185)
Each Party shall adopt such legislative and other measures as may be

necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the input, alteration, deletion, or suppression of computer data, resulting in inauthentic data with the intent that it be considered or acted upon for legal purposes as if it were authentic, regardless whether or not the data is directly readable and intelligible. A Party may require an intent to defraud, or similar dishonest intent, before criminal liability attaches.

a-2) Interference with business transaction by computer system

Article 234-2 of the Penal Code prohibits any interference with business transaction by computer system.

Article 234-2 Interference with business transaction by computer system
Any person who intentionally and knowingly, illegally, causes disruption or interference with regular execution of valid performance of computer system which is being used or intended to be use for business transactions of others, or causes executions which are contrary to proper using or purposes of such computer system, by destruction of such computer system or electromagnetic record which is being used or intended to use in such computer system, by introducing false information or wrong instructions into such computer system, or by the other similar means, and causes interference with business transactions of others shall be punished with penal servitude for not more than 5 years or be fined not more than 100,000yen.

This Article is same to the system interference in the Cybercrime Convention Article 5.

Article 5 System interference (ETS 185)
Each Party shall adopt such legislative and other measures as may be

necessary to establish as criminal offences under its domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

a-3) Computer Fraud

Article 246-2 and 250 of the Penal Code prohibits any computer fraud.

Article 246-2 Computer Fraud
Any person who intentionally and knowingly, illegally, obtain unlawful profit or cause to be obtain unlawful profit to any others, by introducing false information or wrong instructions into computer system which is being used or intended to be use for business transactions of others, by producing false electromagnetic record relating to take, loss or change of property of others, or by using such false electromagnetic record on any business transactions, shall punished with penal servitude for not more than 5 years.

Article 250 Attempt to commit fraud or threatening
Any person who attempts to commit any crimes as set forth in this chapter shall be punishable.

This article is same to the computer-related fraud in the Cybercrime Convention Article 8.

Article 8 Computer-related fraud (ETS 185)
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the causing of a loss of property to another person by:

a) any input, alteration, deletion or suppression of computer data;

b) any interference with the functioning of a computer system,

with fraudulent or dishonest intent of procuring, without right, an economic benefit for oneself or for another person.

a-4) Destruction of electromagnetic record

Article 258, 259 and 264 of the Penal Code prohibits any destruction of electromagnetic record.

Article 258 Destruction of official electromagnetic record

Any person who destroys any documents or electromagnetic record which ought to be use at State office shall be punished with penal servitude for more than 3 months and not more than 5 years.

Article 259 Destruction of private electromagnetic record

Any person who destroys any documents or electromagnetic record relating to take, loss or change of property of others shall be punished with penal servitude for not more than 5 years.

Article 264 Prosecution

Anyone who commits any crimes as set forth in Section 259 or Section 261 shall not be prosecuted without any accusation by victim.

a-5) Problem

This article is same to the data interference in the Cybercrime Convention Article 4, if Japan would reserve the right to require in accordance with Article 8 paragraph 2 of the Cybercrime Convention, due to Article 259 can be applied to serious crimes only.

Article 4 Data interference (ETS 185)

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.
2 A Party may reserve the right to require that the conduct described in paragraph 1 result in serious harm.

On the other hand, the Cybercrime Convention (ETS 185) provides two other cybercrimes in Article 3 and 6.

Article 3 Illegal interception (ETS 185)
Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

Article 6 Misuse of devices (ETS 185)
1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right:
a) the production, sale, procurement for use, import, distribution or otherwise making available of:
i) a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;

ii) a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5; and

b) the possession of an item referred to in paragraphs a.i or ii above, with intent that it be used for the purpose of committing any of the offences established in Articles 2 through 5. A Party may require by law that a number of such items be possessed before criminal liability attaches.

2 This article shall not be interpreted as imposing criminal liability where the production, sale, procurement for use, import, distribution or otherwise making available or possession referred to in paragraph 1 of this article is not for the purpose of committing an offence established in accordance with Articles 2 through 5 of this Convention, such as for the authorised testing or protection of a computer system.

3 Each Party may reserve the right not to apply paragraph 1 of this article, provided that the reservation does not concern the sale, distribution or otherwise making available of the items referred to in paragraph 1 a.ii of this article.

There is no Japanese law which has been directly and clearly addressed these Articles in the Cybercrime Convention. In fact some laws can be interpreted so[3], but there are many opposite opinions among legal scholars. New legislations may be necessary in relation to both these Articles.

b) Unauthorized Access

A specific type of unauthorized access to computer system shall be punished by the Unauthorized Computer Access Law (Law No. 128 of 1999).

[3] For example the telecommunication business law of Japan has a related penalty article which can be applicable to any infringement of secrecy of any being transported data. However such article doesn't directly prohibit any interception of data.

The purpose of this law is in following;

(Purpose)

Article 1. The purpose of this Law is, by prohibiting acts of unauthorized computer access as well as by stipulating penal provisions for such acts and assistance measures to be taken by the Metropolitan or Prefectural Public Safety Commissions for preventing a recurrence of such acts, 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, and, thereby, to contribute to the sound development of the advanced information and telecommunications society.

(Translation by Japan Police Agency)

However all types of illegal access to computer system shall not be punished by this law. This law can prohibit only a specific type of unauthorized access that is any remote access without any right to computer system which has been connected with other computer system.

Article 2 of this law defines in following;

(Definitions)

Article 2. In this law, "access administrator" means a person who administers the operations of a computer (hereafter referred to as "specific computer") which is connected to a telecommunication line, with regard to its use (limited to such use as is conducted through the telecommunication line concerned; hereafter referred to as "specific use").

2. In this Law, "identification code" means a code —

that is granted to a person (hereafter referred to as "authorized user")

who has been authorized by the access administrator governing a specific use of a specific computer to conduct that specific use, or to that access administrator (hereafter in this paragraph, authorized user and access administrator being referred to as "authorized user, etc.") to enable that access administrator to identify that authorized user, etc., distinguishing the latter from another authorized user, etc.; and that falls under any of the following items or that is a combination of a code which falls under any of the following items and any other code:

(1) A code the content of which the access administrator concerned is required not to make known to a third party wantonly;

(2) A code that is compiled in such ways as are defined by the access administrator concerned using an image of the body, in whole or in part, of the authorized user, etc., concerned, or his or her voice;

(3) A code that is compiled in such ways as are defined by the access administrator concerned using the signature of the authorized user, etc., concerned.

3. In this Law, "access control function" means a function that is added, by the access administrator governing a specific use, to a specific computer or to another specific computer which is connected to that specific computer through a telecommunication line in order to automatically control the specific use concerned of that specific computer, and that removes all or part of restrictions on that specific use after confirming that a code inputted into a specific computer having that function by a person who is going to conduct that specific 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; the same shall apply in Article 3, paragraph 2, items (1) and (2)) for that specific use.

(Translation by Japan Police Agency)

And Article 3 of this law prohibits following activities as unauthorized access.

(Prohibition of acts of unauthorized computer access)

Article 3. No person shall conduct an act of unauthorized computer access.

2. The act of unauthorized computer access mentioned in the preceding paragraph means an act that falls under one of the following items:

(1) An act of making available a specific use which is restricted by an access control function by making in operation a specific computer having that access control function through inputting into that specific computer, via telecommunication line, another person's identification code for that access control function (to exclude such acts conducted by the access administrator who has added the access control function concerned, or conducted with the approval of the access administrator concerned or of the authorized user for that identification code);

(2) An act of making available a restricted specific use by making in operation a specific computer having that access control function through inputting into it, via telecommunication line, any information (excluding an identification code) or command that can evade the restrictions placed by that access control function on that specific use (to exclude such acts conducted by the access administrator who has added the access control function concerned, or conducted with the approval of the access administrator concerned; the same shall apply in the following item);

(3) An act of making available a restricted specific use by making in operation a specific computer, whose specific use is restricted by an access control function installed into another specific computer which is connected, via a telecommunication line, to that specific computer, through inputting into it, via a telecommunication line, any information

or command that can evade the restrictions concerned.

(Translation by Japan Police Agency)

Also this law prohibits following activity relating to unauthorized access.

(Prohibition of acts of facilitating unauthorized computer access)

Article 4. No person shall provide another person's identification code relating to an access control function to a person other than the access administrator for that access control function or the authorized user for that identification code, in indicating that it is the identification code for which specific computer's specific use, or at the request of a person who has such knowledge, excepting the case where such acts are conducted by that access administrator, or with the approval of that access administrator or of that authorized user.

(Assistance, etc., by Metropolitan and Prefectural Public Safety Commissions)

Article 6. The Metropolitan or Prefectural Public Safety Commission (each of the Area Public Safety Commissions in case of the Areas (that means the Areas mentioned in Article 51, paragraph 1, main part, of the Police Law (Law No. 162 of 1954); the same shall apply hereafter in this paragraph) except the Area which comprises the place of the Hokkaido Prefectural Police Headquarters: the same shall apply hereafter in this Article), in case an act of unauthorized computer access is recognized to have been conducted and if, for the purpose of preventing a recurrence of similar acts, assistance is requested by the access administrator of the specific computer involved in that act of unauthorized computer access, attaching to such request any documents or articles regarding referential matters, such as the situations of operation and management of that specific computer at the time of that act of unauthorized access, shall

provide, when it deems such request reasonable, that access administrator with assistance, including provision of relevant materials, advice and guidance, so that necessary emergency measures can be properly taken in accordance with the modus operandi of that act of unauthorized access or its cause to protect that specific computer from acts of unauthorized access.

2. The Metropolitan or Prefectural Public Safety Commission may entrust to a person to be stipulated by National Public Safety Commission Regulation with all or part of the work of implementing a case analysis (which means making a technical study and analysis on the modus operandi of the act of unauthorized computer access relating to that request and the cause of such act; the same shall apply in the following paragraph) which is necessary for the providing of the assistance mentioned in the preceding paragraph.

3. A person who has engaged in the work of implementing a case analysis entrusted by the Metropolitan or Prefectural Public Safety Commission in accordance with the preceding paragraph shall not reveal secret he or she has learned with regard to such implementation.

4. The necessary matters, other than those stipulated in the preceding three paragraphs, relating to the assistance mentioned in the first paragraph shall be stipulated by National Public Safety Commission Regulation.

(Translation by Japan Police Agency)

Finally following activities shall be punished under Article 8 and 9 of this law.

(Penal provisions)

Article 8. A person who falls under one of the following items shall be punished with penal servitude for not more than one year or a fine of not

more than 500,000 yen:

(1) A person who has infringed the provision of Article 3, paragraph 1;

(2) A person who has infringed the provision of Article 6, paragraph 3.

Article 9. A person who has infringed the provision of Article 4 shall be punished with a fine of not more than 300,000 yen.

(Translation by Japan Police Agency)

Thus following behavior without right shall not be punished under this law.

1) Any access to stand alone computer systems

2) Any direct access to any computer systems (for instance any access direct from keyboard of such computer system)

3) Any access to any computer systems which any access control function has not been added

However the Cybercrime Convention (ETS 185) has following definition article and substantive criminal law article.

Article 1 Definitions (ETS 185)

For the purposes of this Convention:

"computer system" means any device or a group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data

Article 2 Illegal access (ETS 185)

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed

by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system.

In accordance with definition, unauthorized access to any stand alone computer also shall be punished by law. So there is a kind of lack of law in the current unauthorized Computer Access Law in Japan.
On this problem, the Japanese government may interpret that current law has been addressed to the Cybercrime Convention by limited conditions in current law are all adequate to any additional requirements involved in Article 2 of the Cybercrime Convention. However, current law has a requirement of "via telecommunication line" in Article 3 Section2 (1). This requirement may reject any non-remote unauthorized access from punishable activities by current law, despite most business companies have urged that such non-remote unauthorized access also shall be punished by law[4].

2.2 Other Cybercrimes

The Cybercrime Convention provides also other cybercrimes, the Child pornography and the Infringement of the Intellectual Properties.

a) Digital Pornography and Child Pornography

In Japan, there are two laws relating to the digital pornography, the Penal Code of Japan and the Law for Punishing Acts Related to Child Prostitution and Child Pornography, and for Protecting Children (Law No.52 of 1999).

a-1) Distribution of obscenities

The penal Code of Japan prohibits any distribution of obscenities.

[4] Current unauthorized access law doesn't cover some kinds of new important technology such as electronic tags including RFID (Radio Frequency ID), because such devices (computer systems) are not often connected with any telecommunication line and are similar to stand alone computers. Any direct access by electromagnetic radiation is not involved in the unauthorized access under the current law.

(Distribution of obscenities)

Article 175

Any person who distributes, sells or publicly displays an obscene writing, picture or other materials shall be punished with penal servitude for not more than two years or be fined not more than two million and a half yen or minor fine. The same shall apply to any person who possesses the same with the intention of selling it.

However, there is no definition clause for the term "obscenities" in this Code. So there have been many severe discussions on the interpretation of this Article. Most scholars urge that this Article doesn't include digital pornography because this Article enacted in 1907. There was no digital content at the time at all, and any member of the National Diet could never imagine such digital contents.

Despite such discussions, the Supreme Court of Japan decided an opposite result that any hard disk drives which any pornographic data stored in shall be deemed as obscenities[5].

a-2) Child pornography

The Law for Punishing Acts Related to Child Prostitution and Child Pornography and for Protecting Children (Law No.52 of 1999) provides a prohibition of any child pornography. This law was enacted as an implementation of the Convention on the Rights of the Child (United Nations on 20 November 1989).

Distribution of any child pornography shall be punished under Article 7 and 10 of this law.

Article 7 Distribution, etc. of Child Pornography

1. A person who distributes, sells, lends as a business, or displays in

[5] The Supreme Court Judgment, July 16 2001 (No. 1221-1999)

public, child pornography shall be punished with imprisonment with labor for not more than three years or a fine not exceeding three million yen.

2. A person who produces, possesses, transports, imports to or exports from Japan child pornography for the purpose of conducting any of the acts mentioned in the preceding paragraph shall be punished with the same penalty as is described in the said paragraph.

3. A Japanese national who imports to or exports from a foreign country child pornography for the purpose of conducting any of the acts mentioned in paragraph 1 of this article shall be punished with the same penalty as is described in the said paragraph.

Article 10 Crimes Committed by Japanese Nationals Outside Japan

The crimes specified in Articles 4 to 6, paragraphs 1 and 2 of Article 7, and paragraphs 1 and 3 (limited to the part thereof which relates to paragraph 1) of Article 8 shall be dealt with according to the provision of Article 3 of the Penal Code (Law No. 45 of 1907).

(Translation by Japan Police Agency[6])

However there are many court rulings that are confusing each other on the interpretation of this law, due to some ambiguousness of aims and expression in definition clause of this law. Especially, on the interpretation of aims of this law, most courts believe that the main aim is to prohibiting pornographic materials but not to protect the rights of the Child, and many political people think and urge that such victim children also have to be punished by law as a criminal but not to be protected ant to be given a good education.

Also, this law doesn't address to the Cybercrime Convention partly, especially on distributing through computer system in Article 9 paragraph 1 and sub paragraphs (b) and (c) in paragraph 2. Japanese government may

[6] http://www.npa.go.jp/safetylife/syonen/law.htm

reserve the right not to apply paragraph 1, paragraphs (b) and (c).

Article 9 Offences related to child pornography (ETS 185)

1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally and without right, the following conduct:

a) producing child pornography for the purpose of its distribution through a computer system;

b) offering or making available child pornography through a computer system;

c) distributing or transmitting child pornography through a computer system;

d) procuring child pornography through a computer system for oneself or for another person;

e) possessing child pornography in a computer system or on a computer-data storage medium.

2 For the purpose of paragraph 1 above, the term "child pornography" shall include pornographic material that visually depicts:

a) a minor engaged in sexually explicit conduct;

b) a person appearing to be a minor engaged in sexually explicit conduct;

c) realistic images representing a minor engaged in sexually explicit conduct.

3 For the purpose of paragraph 2 above, the term "minor" shall include all persons under 18 years of age. A Party may, however, require a lower age-limit, which shall be not less than 16 years.

4 Each Party may reserve the right not to apply, in whole or in part, paragraphs 1, sub-paragraphs d. and e, and 2, sub-paragraphs b. and c.

b) Copyright

Any infringement of digital copyright shall be punished by the Copyright Law of Japan.

Article 119. The following shall be punishable by imprisonment for a term not exceeding three years or a fine not exceeding three million Yen:

(i) any person who infringes moral rights of authors, copyright, right of publication, moral rights of performers or neighboring rights (excluding those who reproduce by themselves works or performances, etc. for the purpose of private use as mentioned in Article 30, paragraph (1) (including the case where its application mutatis mutandis is provided for under the provision of Article 102, paragraph (1)) or who does an act considered to constitute infringements on moral rights of authors, copyright, moral rights of performers or neighboring rights (including the rights considered as neighboring rights in accordance with the provisions of Article 113, paragraph (4); the same shall apply in Article 120bis, item (iii)) under Article 113, paragraph (3);

(ii) any person who, for profit-making purposes, causes others to use automatic reproducing machines mentioned in Article 30, paragraph (1), item (i) for such reproduction of works or performances, etc. as constitutes an infringement on copyright, right of publication or neighboring rights.

Article 120. Any person who violates the provision of Article 60 or Article 101ter shall be punishable by a fine not exceeding three million yen.

Article 120bis. The following shall be punishable by imprisonment for a term not exceeding one year or a fine not exceeding one million Yen;

(i) any person who transfers to the public the ownership of, or lends to the public, manufactures, imports or possesses for transfer of own-

ership or lending to the public, or offers for the use by the public, a device having a principal function for the circumvention of technological protection measures (such a device includes such a set of parts of a device as can be easily assembled) or copies of a program having a principal function for circumvention of technological protection measures, or transmits publicly or makes transmittable such program;

(ii) any person who, as a business, circumvents technological protection measures in response to a request from the public;

(iii) any person who, for profit-making purposes, does an act considered to constitute an infringement on moral rights of authors, copyright, moral rights of performers or neighboring rights under the provisions of Article 113, paragraph (3).

Article 121. Any person who distributes copies of works on which the true name or generally known pseudonym of a non-author is indicated as the name of the author (including copies of derivative works on which the true name or generally known pseudonym of a non-author of the original work is indicated as the name of the original author) shall be punishable by imprisonment for a term not exceeding one year or a fine not exceeding one million Yen.

Article 121bis. Any person who makes, distributes or possesses for distribution copies of commercial phonograms reproduced from any of the following commercial phonograms (including copies of such commercial phonograms and those made through one or more intervening copies) shall be punishable by imprisonment for a term not exceeding one year or a fine not exceeding one million Yen, provided that such making, distribution or possession of copies is made within a period of fifty years from the year following the date of the first fixation of sounds on matrices of phonograms:

(i) commercial phonograms which have been manufactured, by those

engaging in the business of manufacturing commercial phonograms in this country, from matrices of phonograms (except those phonograms falling within any of the four items of Article 8) offered by producers of phonograms;

(ii) commercial phonograms which have been manufactured, by those engaging in the business of manufacturing commercial phonograms outside the jurisdiction of this Law, from matrices of phonograms (except those phonograms falling within any of the four items of Article 8) offered by producers of phonograms who are nationals of any of the Contracting States of the Convention for the Protection of Performers, etc., the members of the World Trade Organization or the Contracting States of the Phonograms Convention ("nationals" includes legal persons established under the law of such State or member and those who have their principal offices in such State or member). Article 122. Any person who violates the provisions of Article 48 or Article 102, paragraph (2) shall be punishable by a fine not exceeding three hundred thousand Yen.

Article 123. (1) In the case of offences under Article 119, Article 120bis, item (ii) and Article 121bis, the prosecution shall take place only upon the complaint of the injured person.

(2) A publisher of an anonymous or a pseudonymous work may lodge a complaint with respect to such work published by him, except in the cases where the proviso to Article 118, paragraph (1) is applicable and where the complaint is contrary to the express will of the author.

Article 124. (1) Where a representative of a legal person (including an administrator of a non-juridical association or foundation) or an agent, an employee or any other worker of a legal person or a person violates the provisions mentioned in any of the following items in connection with the business of such legal person or such person, a fine under any of these items shall be imposed upon such legal person, and a fine under any of

the Articles mentioned in item (ii) shall be imposed upon such person, in addition to the punishment of the offender:

(i) Article 119, item (i) (except parts of the provisions relating to moral rights of the author or the performer): a fine not exceeding a hundred million yen;

(ii) Article 119, item (i) (only parts of the provisions relating to moral rights of the author or the performer) or (ii), or Article Article 120 to Article 122: a fine under any of these Articles.

(2) In the case where the provision of the preceding paragraph applies to a non-juridical association or foundation, its representative or administrator shall represent such association or foundation with regard to proceedings, and the provisions of the Code of Criminal Procedure which are applicable when a legal person is the accused or the suspect shall apply mutatis mutandis.

(3) In the case of paragraph (1), a complaint lodged against an offender or the withdrawal of such complaint shall be effective also with respect to the legal person or the person concerned, and a complaint lodged against a legal person or a person or the withdrawal of such complaint shall be effective also with respect to the offender concerned.

(Translation by the Copyright Research and Information Center (CRIC))

In relation to the digital contents, the Copyright Law of Japan provides enough protections.

(Right of preserving the integrity)

Article 20. (1) The author shall have the right to preserve the integrity of his work and its title against any distortion, mutilation or other modification against his will.

(2) The provision of the preceding paragraph shall not apply to the fol-

lowing modifications:

(i) change of ideographs or words or other modifications deemed unavoidable for the purpose of school education in the case of the exploitation of works under the provisions of Article 33, paragraph (1) (including the case where its application mutatis mutandis is provided for under the provision of paragraph (4) of the same Article) and Article 34, paragraph (1);

(ii) modification of an architectural work by means of extension, rebuilding, repairing, or remodeling;

(iii) modification which is necessary for enabling to use on a particular computer a program work which is otherwise unusable on that computer, or to make more effective the use of a program work on a computer;

(iv) other modifications not falling within those mentioned in the preceding three items, which are deemed unavoidable in the light of the nature of a work as well as the purpose and the manner of exploiting it.

Subsection 3 Rights Comprised in Copyright

(Right of reproduction)

Article 21. The author shall have the exclusive right to reproduce his work.

(Right of performance)

Article 22. The author shall have the exclusive right to perform his work publicly ("publicly" means for the purpose of making a work seen or heard directly by the public; the same shall apply hereinafter).

(Right of presentation)

Article 22bis. The author shall have the exclusive right to present his work publicly.

(Rights of public transmission, etc.)

Article 23. (1)The author shall have the exclusive right to make the public transmission of his work (including the making transmittable of his work in the case of the interactive transmission).

(2)The author shall have the exclusive right to communicate publicly, by means of a receiving apparatus, his work of which the public transmission has been made.

(Translation by the Copyright Research and Information Center (CRIC))

Also the Copyright Law of Japan has some Articles relating to infringement and damages.

(Right of demanding cessation)

Article 112. (1) Against those who infringe or are likely to infringe moral rights of authors, copyright, right of publication, and the performers or neighboring rights, the authors as well as the owners of these rights may make a demand for cessation or prevention of such infringements.

(2) In making such demand, the authors, the owners of copyright, the owners of right of publication, the performers or the owners of neighboring rights may demand to take measures necessary to effect such cessation or prevention of infringement, such as the abandonment of objects the making of which constituted an infringement, objects made by an infringement or implements and tools used solely for an infringement.

(Acts considered to be infringements)

Article 113. (1) The following acts shall be considered to constitute infringements on moral rights of authors, copyright, right of publication, moral rights of performers or neighboring rights:

(i) the importation into this country, for distribution, of objects made by an act which would constitute an infringement on moral rights of authors, copyright, right of publication, moral rights of performers or

neighboring rights if they were made in this country at the time of such importation;

(ii) the distribution or the possession for distribution of objects made by an act infringing moral rights, copyright, right of publication or neighboring rights (including those imported as mentioned in the preceding item) by a person who is aware of such infringement.

(2) An act of using on a computer, in the conduct of business, copies made by an act infringing copyright in a program work (including copies made by the owner of such copies in accordance with the provision of Article 47bis, paragraph (1) as well as copies of a program work imported as mentioned in item (i) of the preceding paragraph and copies made by the owner of such imported copies in accordance with the provision of Article 47bis, paragraph (1)) shall be considered to constitute an infringement on that copyright, so long as a person using such copies is aware of such infringement at the time when he has acquired an authority to use these copies.

(3) The following acts shall be considered to constitute infringements on moral rights of authors, copyright, moral rights of performers or neighboring rights relating to rights management information concerned:

(i) the intentional addition of false information as rights management information;

(ii) the intentional removal or alteration of rights management information excluding the case where such act is conditional upon technology involved in the conversion of recording or transmission systems or other cases where it is deemed unavoidable in the light of the purpose and the manner of exploiting works or performances, etc.;

(iii) the distribution, importation for distribution or possession for distribution of copies of works or performances, etc. by a person who knows that any act mentioned in the preceding two items has been done

concerning such works or performances, etc. or the public transmission or making transmittable of such works or performances, etc. by such person.

(4) For the application of the provisions of the preceding paragraph, the right to secondary use fees mentioned in Article 95, paragraph (1) and Article 97, paragraph (1) and the right to remuneration mentioned in Article 95ter, paragraph(3) and Article 97ter, paragraph (3) shall be considered as neighboring rights. In this case, "the owners of neighboring rights" in the preceding Article shall read "the owners of neighboring rights (including the owners of the rights considered as neighboring rights in accordance with the provisions of paragraph (4) of the next Article)", and "neighboring rights" in paragraph (1) of the preceding Article shall read "neighboring rights (including the rights considered as neighboring rights in accordance with the provisions of paragraph (4) of the next Article)".

(5) An act of exploitation of a work prejudicial to the honour or reputation of the author shall be considered to constitute an infringement on his moral rights.

(Exceptional provisions to the right of transfer of ownership in relation to a bona fide third party)

Article 113bis. When the ownership of the original or copies of works (excluding copies of cinematographic works (including copies of cinematographic works in cases of works reproduced in cinematographic works); the same shall apply hereinafter in this Article), sound or visual recordings of performances or copies of phonograms has been transferred to a person who does not know or has no negligence in not knowing that such original or copies of works, sound or visual recordings of performances or copies of phonograms do not fall within any of the items of Article 26bis, paragraph (2), Article 95bis, paragraph (3) or Article 97bis, paragraph (2), respectively, an act by such person to transfer to the public the ownership

of such original or copies of works, sound or visual recordings of performances or copies of phonograms shall be considered not to constitute an infringement on the rights mentioned in Article 26bis, paragraph (1), Article 95bis, paragraph (1) or Article 97bis, paragraph (1).

(Presumption of the amount of damages)

Article 114. (1) In the case where an owner of copyright, right of publication or neighboring rights claims compensation for damages from a person who has infringed intentionally or negligently any of these rights, the profits, if any, obtained by the infringer from that infringement shall be presumed to be the amount of damages suffered by such owner.

(2) The owners of copyright and neighboring rights may claim compensation for damages from a person who has infringed intentionally or negligently their copyright or neighboring rights, the amount of damages suffered being that corresponding to the amount of money which would be received by them through the exercise of these rights.

(3) The provision of the preceding paragraph shall not prejudice any claim to compensation for damages in excess of the amount mentioned therein. In such case, the court may consider the absence of any bad faith or gross negligence on the part of the infringer in fixing the amount of damages.

(Translation by the Copyright Research and Information Center (CRIC))

This Copyright Law has been addressed to the Cybercrime Convention completely.

Article 10 Offences related to infringements of copyright and related rights (ETS 185) 1 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of copyright, as defined under the law of that Party, pursuant to the obligations it has undertaken under the Paris

Act of 24 July 1971 revising the Bern Convention for the Protection of Literary and Artistic Works, the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Copyright Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

2 Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law the infringement of related rights, as defined under the law of that Party, pursuant to the obligations it has undertaken under the International Convention for the Protection of Performers, Producers of Phonograms and Broadcasting Organisations (Rome Convention), the Agreement on Trade-Related Aspects of Intellectual Property Rights and the WIPO Performances and Phonograms Treaty, with the exception of any moral rights conferred by such conventions, where such acts are committed wilfully, on a commercial scale and by means of a computer system.

3 A Party may reserve the right not to impose criminal liability under paragraphs 1 and 2 of this article in limited circumstances, provided that other effective remedies are available and that such reservation does not derogate from the Party's international obligations set forth in the international instruments referred to in paragraphs 1 and 2 of this article.

3. Problems; Analysis and Perspectives

I have presented a total structure of the cybercrime legislation of Japan and pointed out the existence of many problems in previous section.

These problems have been generated mainly from the absence of a uniform legislation policy. In fact it may be very difficult to establish such uniform policy. Probably only few people are able to observe current phenomena

correctly and well establish such policy, because the Internet itself has been changed continuously and related interests may be also very complicated and fluid.

In addition most of the National Diet members would have not had enough interests in any legal issues on the Internet.

However I believe that a good uniform policy for cyber legislation shall be established because of following reasons.

1) To be clear

In fact there may be different legislation policies in each country. It may be not avoidable.

However it is very important to be clear any differences between such legislation policies. If any differences would not be clear then one can not discover and discuss about important international problems and any improvement of such policies would be hopeless.

2) To reject complexity and duplication of legislation

If such complexity and duplication of legislation could not be rejected then law enforcement would also be so and more dangerous problems would be taken place (for instance double jeopardy).

On the other hand complexity and duplication may generate some conflicts between relevant laws, and would bring ambiguousness of application scope and lacks of laws. If one can't know such application scope of laws then no one can imagine what is lawful or what is illegal. A lack of the foreseeable condition would bring a social instability.

3) To be criticized

Due to the incomplete nature of human being itself, every legislation policy would always involve some misjudgment. This may be unavoidable

until the end of human civilization.
However if any policies can be criticized by the citizen then such misjudgments can be corrected and be exchanged for better policies. It has been one of the basic principles of the democracy. So written and clear policy should be established and presented to the citizen also in the area of cyberlaw.

So we have to examine more and more what is the better way to resolve complicated problems which have been taken place on the Internet.

As a conclusion, I would like to propose some requirements that should be taken account at the establishment of such uniform legislation policy.

1) To indicate considered values or interests
2) To make good balance between such values and interests
3) To present superior value or interest and to explain its reason
4) To propose better constitution of Japan

4. Conclusions

There are many fundamental cybercrime laws in Japan. However, some important lacks can be found in Japanese legislations, especially in relation to the Cybercrime Convention, many problems remain.
Thus more studies and examinations relating to the existing laws and international instruments on cybercrimes have to be done.
As well as, more clear legislation policy has to be established, especially relating to cyber legislations.