CYBERCRIMES IN JAPAN: RECENT CASES, LEGISLATIONS, PROBLEMS AND PERSPECTIVES[1]

Takato Natsui
Professor at Faculty of Law
Meiji University, Tokyo, Japan

Abstract

Cybercrimes and computer crimes have been taking place on the Internet since 1970s. On the other hand, traditional crimes by means of new technologies are also increasing. Of course, some of such behaviors should be punishable by current criminal laws, and there are many court rulings relating to Cybercrimes in Japan. However some of such behaviors are not covered by existing laws of Japan. Especially unauthorized access to stand alone computers is not punishable by existing laws. On March 2003, the Minister of the Ministry of Justice of Japan consulted with the advisory committee on some amendments relating to Cybercrimes and relevant criminal procedures. This report presents an overview of current legislation and cases relating to Cybercrimes in Japan, introduces recent legislative discussions and points out some problems involved in such legislation and court rulings[2].

Keywords

Cybercrime, cyberlaw, information society, the Internet, legislation, court ruling, Japan

Introduction

Since the 1970s, electronic data processing by computer systems had been introduced into ordinary business areas also in Japan. Most such systems were so-called stand alone systems or small internal network systems that were used only inside private companies. In some important areas, external network systems had been developed and introduced. Especially, computer systems of banks were connected with each other by a common network system for the purpose of electronic money sending or other important electronic transactions. At the same time, computer crimes and so-called white-collar crimes which were committed by using computer systems had been taking place.

However in some cases, due to an absence of law, some wrong activities can not be punished by laws. Data theft is one of the most important examples. The first court case[3] relating to a computer crime in Japan was such a data theft case [Case 1][4].

---

[1] This report is based on my previous article, "*The Recent Cybercrime Legislations in Japan*", Meiji Law Journal vol.10 pp.1-34, March 2003. This previous article doesn't include any cases, statistics and explanation of the consultation by the Minister of the Ministry of Justice on March 2003 at all. Furthermore, I reconstructed the previous article and added many detailed explanations in this report.

[2] About the legal information in Japan, please refer "*How to Conduct a Search for Japanese Translation of Foreign Laws*" by Osamu Miura (SHIP project Review 2003-a pp.131-138).
http://ship.mind.meiji.ac.jp/lib/2003-a.pdf
This article presents mainly a measure to retrieve a Japanese translation of foreign laws, but also presents a measure to search legal information of Japan in general.
And to research English translated legal information of Japan, following Web Sites are very useful.
Links on Japanese Law by the Network Committee of Tohoku University School of Law
http://www.law.tohoku.ac.jp/tohokulaw2.html
Links to Laws of Japan by Takato Natsui
http://www.isc.meiji.ac.jp/~sumwel_h/links/linkJ04.htm
In addition, the Ministry of Public Management, Home Affairs, Posts and Telecommunications (Somusho) provides a database service where all laws and regulation of Japan can be retrieved in Japanese.
http://law.e-gov.go.jp/cgi-bin/idxsearch.cgi

[3] In Japan, court rulings have been published through official case books as well as case journals which have been published by private publishers (for instance, Hanrei Times Corporation and Hanrei Jiho Corporation). So everyone has to retrieve not only the official case books but also such private case journals. Most cybercrimes cases are involved in such summary judgments, and the Summary Court judges usually sentences a small fine. However, most summary judgments by Summary Courts can not be retrieved at all, due to the fact that most summary judgments could not be published officially.

[4] Most court cases are not translated into English. Only the summaries of Supreme Court cases (English translation) can be found at the Web Site of the Supreme Court of Japan.
http://courtdomino2.courts.go.jp/home.nsf/ehome?OpenPage

[Case 1]

ATENA Corporation vs. the Nagano Computer Center (Judgment, 19 February 1973, case number; Showa 46 WA Civil 4095, Tokyo District Court [5][6])

The first case relating to computer crime in Japan was filed in 1973 at the Tokyo District Court. This case was a civil damage case, not a criminal case. But the main argument of this case was purely data theft. Nikkei McGraw-Hill was the joint company of Nikkei Shinbun (a famous news company in Japan) with McGraw-Hill at the time.

(FACTS)

ATENA Corporation (plaintiff) is a postal Tag printing company and the Nagano Computer Center (defendant) is a computer data processing company. Plaintiff received a request of printing customers' address and name on paper Tags from Nikkei McGraw-Hill (a famous publisher). In 27 October 1970, an employee of plaintiff brought some electromagnetic tapes into the defendant's factory at Sinjuku, Tokyo. Customer data of Nikkei McGraw-Hill was recorded in these electromagnetic tapes. The data should be printed out on paper Tags at the factory, and his job was to watch this processing. His job was a confidential job, and he had to protect these electromagnetic tapes and recorded customer data from any data thefts. These printed Tags had to be used only for sending publications of Nikkei McGraw-Hill via the Japan Postal Office. However the employee slept deeply for a while in the factory. While he was sleeping, the customer data was copied by someone without any permission. He finished his job in 28 October 1970, but the employee couldn't recognize that such unauthorized data copying took place.

After that, in January 1971, Nikkei McGraw-Hill discovered that the same customer data was using on the postal Tags printed by Readers Digest Japan. Nikkei McGraw-Hill suspected that Readers Digest Japan stole the customer data by copying from the electromagnetic tapes at the defendant's factory, and accused Readers Digest Japan. However the Japan Police Agency refused receiving this accusation, because any data theft should not be punished by existing law at the time. In addition, Nikkei McGraw-Hill couldn't discover any clear evidence to prove that Readers Digest Japan stole the customer data of Nikkei McGraw-Hill.

(CLAIMS)

Thus, plaintiff compensated all damages caused by this trouble to Nikkei McGraw-Hill, and sued defendant.

Amount of sued damage was 4,569,484 Japanese Yen.

As a cause of action, plaintiff asserted that a defendant's failure of preventing any data theft in the factory was equal to a mishandling of plaintiff's data recorded in the electromagnetic tapes, and that this mishandling caused the damages of Nikkei McGraw-Hill and plaintiff.

(JUDGMENT)

The Tokyo District Court ordered the defendant to compensate a part of plaintiff's damage (2,039,420 Japanese Yen) and costs.

After this case took place, some malicious activities took place relating to computer systems. This was not only in Japan but also in all industrially advanced nations[7]. People discussed computer crime and white-collar crime by means of computer technology. As a result, people recognized the danger of such crimes or malicious activities, and the Penal Code of Japan was amended in 1987. This amended Penal Code has some provisions to ban such activities and punish them as important computer crimes.

Since 1995, the Internet has been continuously growing up. The Internet has been used for various purposes as a common measure to connect a computer system with another computer system. Currently the Internet is the most important infrastructure in our daily life. Numerous people are enjoying the

---

English translations of court cases in this report are all translated by Takato NATSUI, except Supreme Court judgment.

[5] Hanrei Times, no.289 p.155

[6] In Japan, in general, the Supreme Court is the highest court, the High Court is an appeal court and the District Court is the lowest court. On family cases (for instance divorce conciliation and juvenile crime cases), the Family Court is the first step court. There is only one Supreme Court, six High Courts and about fifty District Courts as well as many branch Courts in Japan. Further, there are many Summary Courts for small cases both civil and criminal. A summary judgment means a court ruling ordered only at the Summary Court that is not same as a summary judgment in the US.

[7] The first book on computer crime published in Japan is "Computer Crime", 1977, Shujun-sha. This book is a Japanese translation of Don B. Parker's "Crime by Computer", 1976. Mr. Sabro Haneda translated this book.

Internet for many different purposes, for instance sending emails, retrieving information, publishing their articles, enjoying games, making friends, seeking new customers, getting money and binding business contracts and so on.

However criminal people also can be users of the Internet.

Cybercrimes are taking place on the Internet, for instance, computer hacking (unauthorized access to computer systems), ID theft (identification information theft), interference with and destructions of computer systems by DoS (Distributed Denial of Service) attack or by distribution of computer viruses, unauthorized data modification, digital copyright infringement, cyber squatting (misuse of domain names), privacy intrusion, various types of defamation on the Web, network fraud, SPAM (unsolicited bulk advertisement email messages for commercial purpose), distribution of child pornographies, misuse of law enforcement power (illegal interception of people's telecommunication by officials). These have been becoming a serious concern for many people.

This is the most surprising change. Ordinary people can access every computer systems connected with the Internet all over the World, but criminal people can do so too. The internet is a great communication tool for ordinary people, but at the same time it is a powerful and dangerous tool for criminal people.

Due to such a big change, 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.

For example, the Japan Police Agency announced officially the number of arrested people and the number of related complaints[8]. Table1 indicates increasing malicious activity on the Internet and other computer network systems including mobile phone related complaints in the past three years.

	2002	2001	2000
Auction on the computer network	3,978	2,099	1,301
Fraud and related malicious trading	3,193	1,963	1,396
Defamation	2,566	2,267	1,884
Malicious contents	2,261	3,282	2,896
Unsolicited e-mail message	2,130	2,647	1,352
Unauthorized access, computer virus etc.	1,246	1,335	505
Others	3,955	3,684	1,801
Total	19,329	17,277	11,135

Table1: the number of complaints relating to Cybercrime

Also Table 2 shows an increase in the total number of arrested people in the past three years.

	2002	2001	2000
Unauthorized computer access	51	35	31
Computer crimes on Penal Code	30	63	44
(Illegal electromagnetic record)	(8)	(11)	(9)
(computer interference)	(4)	(4)	(2)
(computer Fraud)	(18)	(48)	(33)
Other crimes by means of network systems	958	712	484
(prostitution of children)[9]	(268)	(117)	(8)
(child pornography)	(140)	(128)	(113)
(fraud)	(112)	(103)	(53)
(obscenities)[10]	(109)	(103)	(154)
(Intimidation)	(33)	(40)	(17)
(copyright infringement)	(31)	(28)	(29)
(defamation)	(27)	(42)	(30)
Total	1,039	810	559

Table 2: the number of arrested persons relating to computer crimes

[8] Press release on 20 February 2003 by Japan Police Agency (in Japanese) http://www.npa.go.jp/hightech/arrest_repo/kenkyo_2003_.pdf

[9] The prostitutions of children have been taking place mainly at the meeting points on the Web or via mobile phones.

[10] This number doesn't include the number of the child pornography.

These are current problems which are taking place not only in Japan but also in every other country. All countries are sharing common problems in the same information society. Due to this, similar new laws are enacted and being drafted also in other countries, and many international treaties and agreements relating to the Internet have been bound between Japan and other countries, for instance the European Council Cybercrime Convention of 2001 (ETS no.185)[11], WIPO new Copyright Treaty of 1996[12]. The party countries of such international instruments have to address the requirements and obligations involved in such international instruments.

In fact there are many difficulties of legislation and law enforcement in the area of cybercrime. There is a lack of laws or delay of legislation to address the information society. On the other hand, there are some misjudgments by courts mainly due to a sort of misunderstanding. These have been caused by mainly judges' misunderstanding or ignorance of the computer technology.

On 24 March 2003, the Minister of the Ministry of Justice (MOJ) consulted a legislative examination with the Advisory Committee on the Legal System. This consultation includes some amendments of the Penal Code and some relevant criminal procedure law to address the Cybercrime Convention. If the amendment bill is enacted then some of these problems can be resolved by the new law, but at the same time other problems may take place.

The aims of this report are to present an overview of current legislation and cases relating to Cybercrimes in Japan, to introduce recent legislative discussions and to point out some problems involved in such legislation and court rulings.

Overview of Cybercrimes Legislation in Japan

In Japan there are many laws relating to the information society, and many scholars believe that such laws are constituents of Cyberlaw[13].

Cyberlaw may include various laws in such areas as electronic government, intellectual property protection (digital copyrights, business patents, domain name etc.), electronic commerce and electronic signature, telecommunication, provider liability, personal data protection or privacy issues, electronic evidence and criminal procedure. Also there are many criminal activities relating to computer systems and computer data. Many scholars believe that such various activities are Cybercrimes too.

The total structure of Cyberlaw in Japan can be illustrated by the following figure. Of course, there are a lot of related administrative laws, regulations and ordinances especially in the area of telecommunication. These are too complicated to explain in short term, but requirements by these regulations are strong standards to regulate a kind of order in the Cyberspace.

And also there are a lot of related industrial standards, for example on a privacy protection (JIS Q 15001[14]) and on a security management (JIS X 5080:2002[15]) in Japan. These industrial standards are not

[11] Convention on Cybercrimes (ETS no. 185, signed in Budapest November 23, 2001)
http://conventions.coe.int/Treaty/EN/WhatYouWant.asp?NT=185
The Japanese government signed the Cybercrime Convention in 23rd of 2001, but this convention has not been accepted and ratified at the National Diet of Japan yet.
[12] WIPO Copyright Treaty (adopted in Geneva on December 20, 1996)
http://www.wipo.int/clea/docs/en/wo/wo033en.htm
Most provisions in the Copyright law of Japan have already been amended in accordance with the related conditions by WIPO Copyright Treaty of 1996.
[13] There is no official definition of what is the "Cyberlaw" at all, but we can discover some definitions of Cyberlaw in many books and articles. These definitions might be different to each other and confusing sometimes. For the purpose of this report, I would like to define the Cyberlaw as a law relating to the Internet and digital data.
[14] JIS Q 15001 is base on ISO/IEC 17799.
See the Web Site of "Privacy Mark System" at JIPDEC.
http://privacymark.org/ref/
[15] JIS X 5080 is based on BS 7799-2:2002
See the Web Site of "Conformity Assessment Scheme for Information Security Management Systems (ISMS)" at JIPDEC.
http://www.isms.jipdec.or.jp/en/

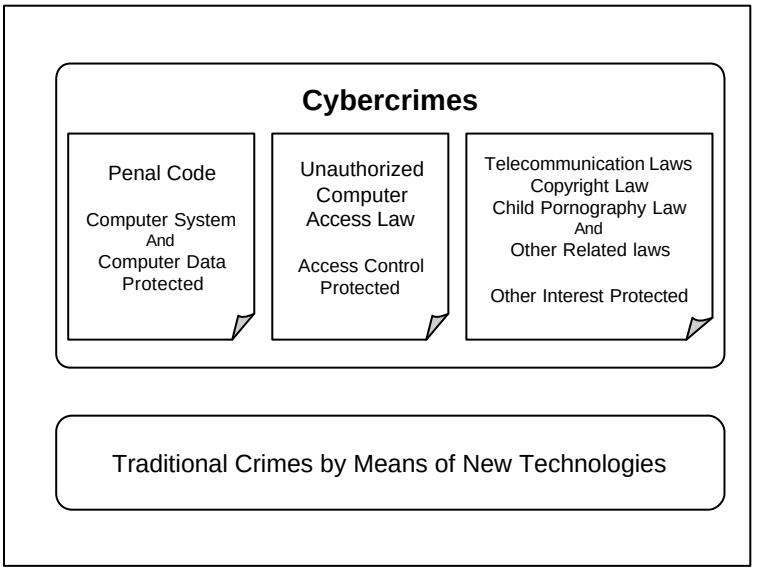
law, but these have a big influence to Japanese companies and related organizations, especially to establish a public policies and self-regulation guidelines.

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

Further, there is no strict penal law on a privacy protection, electronic commerce and consumer protection, except some administrative regulations. This is caused by an absence of a uniform legislation policy on Cyberlaw.

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

Fig.1 Legislation Structure



Main Cybercrimes

Main cybercrimes shall be punished by the Penal Code of Japan (Law No.45 of 1907, amended 1987) and the Unauthorized Computer Access Law (Law no. 128 of 1999).

Most Cybercrimes defined in the Cybercrime Convention (ETS 185) are also punishable by the Penal Code. However the following parts of Cybercrimes involved in the Cybercrime Convention aren't covered by existing laws of Japan yet. Also these activities are not involved in the consultation by the Minister of MOJ on March 2003.

1) Unauthorized access to a stand alone computer system[16]
2) Unauthorized interception of a communication in some areas[17]

Crimes in Penal Code of Japan

The penal Code of Japan enacted in 1907, so of course there was no computer system and computer data at the time. So the Penal Code had been amended in 1987.

The main purpose of this amendment was to ensure a modern computerized business works by prohibiting any computer crimes, especially to protect safety electronic fund transfer transactions and the integrity of computer programs and electronic data. By this amendment, the Penal Code of Japan has

[16] See 2.1.b.2 of this Report
[17] Many scholars urge that such an interception has been covered by the wired telecommunication law, the telecommunication business law and the electronic wave law. However, for instance, an interception of a wireless LAN system inside of an individual's home or private company has not been covered by these laws.

some types of cybercrime articles. On Cybercrimes, the current Penal Code has a definitions provision and covers the following activities to be punishable.

1) Definition of an electronic magnetic record
2) Illegal production of an electromagnetic record
3) Interference with business transaction by computer system
4) Computer fraud
5) Destruction of electromagnetic record

Definition of an electromagnetic record

Similar to other Japanese laws, the Penal Code has a few definition clauses. The only one definition provision relating to computer crimes is Article 7bis.

Article 7bis Definitions
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. And many scholars of Criminal Law regard that 'electromagnetic record' doesn't include a computer program, because a computer program consists of a pure instruction[18] to a computer system but not a record to be processed by a computer system.

I think that this understanding is not right. If such an interpretation is correct, for example, illegal production of a computer program can not be punished by the Penal Code[19]. "Instruction" is a result of an execution of a computer program, not the computer program itself. Most computer programs are stored in the storage media as a digital file, and such a file is an electromagnetic record.

However, in many cases, computer programs would have equal value to or more value than computer data. There is no case on the interpretation of this Article.

Illegal production of an electromagnetic record

Article 161bis of the Penal Code prohibits any illegal production of an electromagnetic record. This Article is the same as the computer-related forgery in the Cybercrime Convention Article 7.

Article 161bis Illegal production and use of an electromagnetic record
Any person who with the intention of misleading any business management of others, illegally produces such an 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 an 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.

"Illegal production" means to produce a new record, to damage an existing record, to modify an existing record and to remove an existing record with the specific intention, except physical destruction of a tangible media on which an electromagnetic record is recorded, is not involved in "Illegal production" of an electromagnetic record.
Relating to this Article, there are many criminal cases. The most cases are of an illegal production and modification of various electromagnetic records which are recorded on electromagnetic strips of various

[18] The Penal Code of Japan clearly distinguishes "record" and "instruction". See. Article 243bis
[19] See Article 161bis.

types of debit cards [See Case 2], service cards and pre-paid card[20] and on the computer systems connected with other computer systems by telephone line [See. Case 3].

On the other hand only "an electromagnetic record relating to legal right, duty of certification of a fact as to be provided for the use of the business management" (private data; Article 161bis paragraph 1) or "electromagnetic record to be made by public offices officers" (official data; Article 161bis paragraph 2) can be protected by the Penal Code. So a simple electromagnetic data which represents only a pure fact (for instance, photos, statistics data, design data etc.) has to be rejected from "electromagnetic record" [See. Case 4].

At any rate, there are not so many cases in Japan, because most relating cases have been accused as a forgery case or counterfeiting securities case. The number of this crime is released by the Japan Police Agency [Table 3]. And some court cases are published [Case 2 and 3].

Year	2002	2001	2000
The number of arrested people	8	11	9

Table 3: the number of illegal electromagnetic record production

[Case 2]
ATM fraud at Fuji Bank and other banks Case (22 February 1989, judgment, case number; Showa 63 WA Criminal 2246, Tokyo District Court)[21]

This criminal case is one of the leading cases of an illegal production of an electromagnetic record on a debit card which can be used at the ATM system of a bank. Substantially, this case is a computer fraud case. The accused made some illegal productions of electromagnetic record as a means for a computer fraud at the ATM system. Fuji Bank was one of the most famous Banks in Japan at the time.

(FACTS)

The accused was a computer engineer. He was studying a computer processing and an operation of ATM system at his office. There were many teller machines, ATM machines and computer systems in his office, these machines were prepared for the purpose of a training course managed by his employer company. So he had much knowledge on the mechanism of the ATM system and the structure of electromagnetic record, and he knew very well that many monitors were watching all customers near the ATM system. But He was heavily in debt. One day he decided to get much money by means of an illegal production of an electromagnetic record on a debit card.
He prepared some plane plastic cards and some small portion of video tape, and he glued the portion of video tape on the plastic cards. After that, he recorded the data of PIN number, bank code, branch code and bank account number on his false cards which by using computer systems in his office.
In 22 -28 June 1988, he went to Fuji Bank and other Banks nine times. He made himself seem a woman to avoid being detected by monitors near the ATM machines at the Banks. He inserted his false plastic cards into the ATM machines, and withdrew money from the ATM machines.
Total amount which he withdrew was 3,625,000 Japanese Yen.

(COUNTS)

Article 161bis - Illegal production of an electromagnetic record
Article 235 - Theft[22]

(JUDGMENT)

Tokyo District Court concluded guilty on all his counts and ordered the accused to be two years and six month penal servitude (imprisonment with compulsory labor) with four years suspension of execution.

[Case 3]
BBS fraud at Nifty-Serve Case (9 May 1997, judgment, case number; Heisei 8 WA Criminal 1226 etc., Kyoto District Court)[23]

[20] On the telephone card case, there were some discussions. Supreme Court of Japan judged that if the surface of the card represents securities then an illegal production of such electromagnetic data shall be punished by Article 162 as a counterfeit of securities (5 April 1991, Kei-shu vol.45 no.4 p.171). In the special case in which the surface of a card doesn't represent securities, Nagoya District Court judged that in such a case Article 161bis should be applied (22 April 1993, Hanrei Times no.840 p.234).
[21] Hanrei Jiho no.1308 p.161
[22] This court judged that the withdrawal by the accused from the ATM machine should be regarded as a theft. But I think that there is a sort of confusion between a theft and a computer fraud (Article 246bis), because the ATM machine is one of the computer systems. If the ATM machine is not a computer system then the withdrawal without any right shall be deemed as a theft. But if the ATM machine is one of the computer systems then the withdrawal without any right shall be interpreted as a computer fraud. Thus this case might be an example of misjudgment by court.

(FACTS)

This criminal case is one of the network fraud cases on the BBS (Bulletin Board Service). Nifty-Serve was the joint company of Nifty Corporation with CompuServe at the time.
The accused had been familiar with a computer technology since his middle school age. He often accessed to a public BBS, and he met a friend (F) on the net. F knew many criminal techniques, especially a technique for committing a fraud by means of computer network systems very well. One day, F taught the accused how to open a fictional bank account to avoid a tracing by police agency.
In January and February 1996, the accused opened two fictional bank accounts. Also he produced some false data including his name and postal address on the Nifty-Serve's database system on 27 March 1996. After that, he wrote some false requests of selling parts of computer systems and related devices at the free market area on the Nifty-Serve BBS on 13 April 1996.
Some ignorant victims believed these false sentences made by the accused and sent money to his false bank accounts on 15-17 April 1996.
Total amount of money sent from victims was about 7,000,000 Japanese Yen.

(COUNTS)

Article 161bis - Illegal production of an electromagnetic record
Article 159 - Forgery of private documents
Article 161 – Uttering of forged private documents
Article 246 - Fraud

(JUDGMENT)

Kyoto District Court concluded guilty on all his counts and ordered the accused to be two years penal servitude (imprisonment with compulsory labor) with three years suspension of execution and probation.

Interference with business transaction by computer system

Article 234bis of the Penal Code prohibits any interference with business transaction by computer system. This Article is the same as the system interference in the Cybercrime Convention Article 5.

Article 234bis 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 the proper use 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.

[Case 4]
Asahi TV Case (3 October 1997, judgment, case number; Heisei 9 WA Criminal 2305, Osaka District Court)[24]

This Criminal Case is one of the most famous computer crime cases in Japan and is classified as a denial of service crime[25]. Substantially, this case might involve an unauthorized access to the Web Server of Asahi TV, but details are not so clear. Asahi TV is a TV broadcast company in Osaka, Japan.

(FACTS)

Asahi TV has been providing current photos of the surface of the earth from the weather observation satellite "Himawari" on its Web Site. On 1997, the accused discovered that the photos on the Web might be exchangeable for other photo data by overwriting the photo data. So he sent some pornography data that had the same names as the names of photo data on the Asahi TV's Web Site on 18 May 1997. As a result, photos of the surface of the earth on Asahi TV's Web Site were exchanged for the pornographies sent by the accused.

[23] Hanrei Jiho no.1613 p.156
[24] Supreme Court (ed.); Card crimes and Computer Crimes Case Book p.216
[25] Some States in the US have the denial of service attack provision in their criminal law. For instance, Pennsylvania Consolidated Statutes title 18 Section 3933 Paragraph 4 provides as follows; intentionally or knowingly engages in a scheme or artifice, including, but not limited to, a denial of service attack, upon any computer, computer system, computer network, computer software, computer program, computer server or data base or any part thereof that is designed to block, impede or deny the access of information or initiation or completion of any sale or transaction by users of that computer, computer system, computer network, computer software, computer program, computer server or data base or any part thereof.

Soon later many visitors discovered this change, and complained to Asahi TV. This caused an Interference with business transaction by Asahi TV's computer system, and Asahi TV stopped its photo providing service on the Web Site.

(COUNTS)

Article 234bis - Interference with business transaction by computer system
Article 175 - Distribution of obscenities

(JUDGMENT)

Osaka District Court concluded guilty on all his counts and ordered the accused to be one year and six months penal servitude (imprisonment with compulsory labor) with three years suspension of execution.

The number of comp uter interference is released by the Japan Police Agency [Table 4][26].

Year	2002	2001	2000
The number of arrested people	4	4	2

Table 4: the number of computer interference

Computer Fraud

Article 246bis and 250 of the Penal Code prohibits any computer fraud. This article is the same as the computer-related fraud in the Cybercrime Convention Article 8.

Article 246bis Computer Fraud
Any person who intentionally and knowingly, illegally, obtain unlawful profit or cause to obtain unlawful profit to any others, by introducing false information or wrong instructions into computer system which is being used or intended to be used for business transactions of others, by producing a 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.

There are many computer fraud cases. Most cases are relating to electronic banking systems, electronic money sending systems and ATM systems. And in many such cases, insiders of Banks had a hand in a plot, so such cases can be classified as one of the white-collar crimes. The number of computer frauds is released by the Japan Police Agency [Table 5][27].

Year	2002	2001	2000
The number of arrested people	18	48	33

Table 5: the number of computer frauds

Destruction of electromagnetic record

Article 258, 259 and 264 of the Penal Code prohibits any destruction of electromagnetic record. These activities mean simple destructions of existing electromagnetic records.

Article 258 Destruction of official electromagnetic records
Any person who destroys any documents or electromagnetic record which ought to be used at a 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.

[26] See also Table 2.
[27] See also Table 2.

If both the destruction of existing electromagnetic record and its modification take place, then only Article 161bis (Illegal production and use of an electromagnetic record) is applicable. Such destruction would be deemed as a part of the illegal production of an electromagnetic record.

Data Theft

Case 1 above is the first published court ruling relating to the computer crime in Japan. Since this case took place, people have been discussing this problem. However there is no law that anyone who commits a data theft shall be punished in Japan. Most scholars of penal law believe that there is no necessity for punishing such an activity.

A famous professor said that a data theft doesn't involve any transference of a tangible property, but only a copying of the data. Of course, if a data is lawfully copyrighted then anyone who copies the data without any permission shall be punished by Copyright Law of Japan. But it seems a little bit funny, I think.
On the other hand, many people including labor unions oppose enacting of ban on data theft. They urged that the ban on data theft would cause a censorship by the police officers as a result.
I think that this problem includes difficult debating points but has a huge influence upon the important social interests to be considered. Including ID theft (for instance, credit card number theft), we have to examine more and more on this problem.

Unauthorized Computer Access

Current law

A specific type of unauthorized access to computer system shall be punished by the Unauthorized Computer Access Law (Law No. 128 of 1999). The purpose of this law is as follows;

Article 1 Purpose

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)[28]

This Article is very complicated. This might be due to the legislative history of this law. So I would like to try to illustrate the structure of this Article by indicating the important items [Fig.2].

Goals:
1) to prevent computer-related crimes
and
2) to maintain the telecommunications-related order that is realized by access control functions

Methods:
1) by prohibiting acts of unauthorized computer access
and
2) by stipulating penal provisions for such acts
and
3) by assistance measures to be taken by the Metropolitan or Prefectural Public Safety Commissions

Results:
to contribute to the sound development of the advanced information and telecommunications society

Fig.2: purposes of law

For the purpose of Goal 1, MOJ governs all criminal behaviour relating to this law, for the purpose of Goal 2 the Ministry of Telecommunication governs all regulations relating to an access control, for the

[28] This translation by Japan Police Agency can be found at the Web Site of the Agency. http://www.npa.go.jp/hightech/fusei_ac2/ucalaw.html

purpose of Results, the Ministry of Telecommunication and the Ministry of Economy, Trade and Industry (METI) co-govern all regulations relating to information industries and telecommunication industries. These are due to a deep complexity of the structure of Japanese government.

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 a computer system which has been connected with another computer system. Article 2 of this law defines as follows;

Article 2 Definitions
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 some activities as unauthorized access. Under this law, only these activities can be regarded as unauthorized access[29].

Article 3 Prohibition of acts of unauthorized computer access
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

[29] The explanatory Report of the Cybercrime Convention (ETS 185) explains at paragraph 45: [t]he most effective means of preventing unauthorised access is, of course, the introduction and development of effective security measures. However, a comprehensive response has to include also the threat and use of criminal law measures. A criminal prohibition of unauthorised access is able to give additional protection to the system and the data as such and at an early stage against the dangers described above.
http://conventions.coe.int/Treaty/en/Reports/Html/185.htm
On an interpretation of "unauthorized access" in the US, See also Orin S. Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 New York University Law Review
http://papers.ssrn.com/sol3/papers.cfm?abstract_id=399740

(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)

This provision is one of the most difficult provisions of all laws. It is not a sort of English translation problem. In fact the original provision in Japanese is also too complicated and full of long sentences to be easily understood by Japanese professional lawyers. So I would like to explain this Article by using some figures.

In general, one might consider that "unauthorized access" means all types of the Hacking activity. Despite such common sense, the scope of "unauthorized access" in this law is not so wide; a protected computer system is limited to "a specific computer", and "a specific computer" means a computer system which is connected to a telecommunication line by the provision of Article 2, also, a protected computer should have an access control function by the provision of Article 3 [Fig. 3].

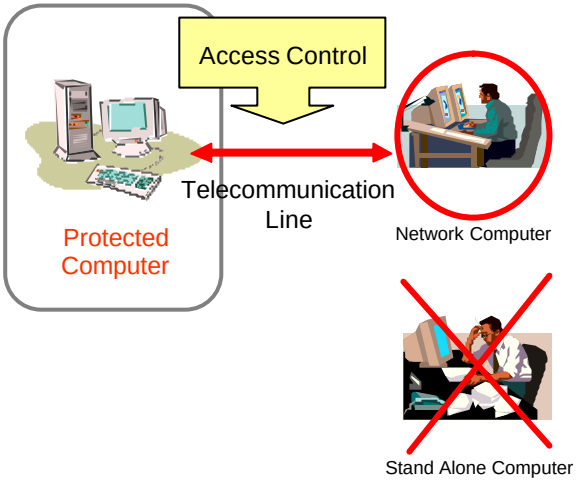


Fig. 3: protected computer

And Article 3 provides three types of unauthorized computer access. Article 3 Paragraph 2 (1) and (2) provide two methods of unauthorized access to break any access control functions [Fig. 4]. Malicious access by means of other methods could not be punished by this law.

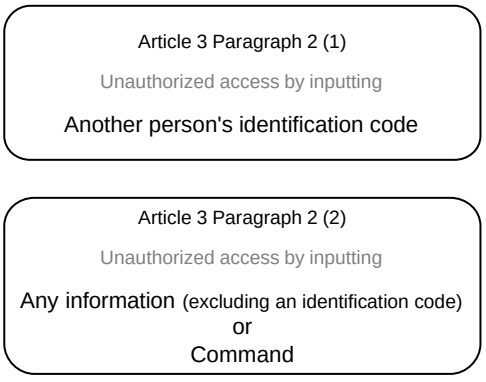


Fig. 4: two methods for unauthorized computer access

The identification code in Article 3 Paragraph 2 (2) is defined at Article 2 Paragraph 2. An example of a code in Paragraph 2 (1) is an access ID and password, a code in Paragraph 2 (2) means a so-called bio-metric identification and Paragraph 2 (3) provides any other ways.

Article 3 Paragraph 2 (3) provides an unauthorized access to a computer (A) which its specific use is restricted by an access control function installed into another specific computer (B) [Fig. 5]. To interpret the requirements of this provision is very hard, but the requirements can be analyzed to follows;

1) Target computer is Computer A [30]
2) Any use of computer A is restricted by Computer B
3) Computer A has an access control function
4) Computer A and Computer B are both specific computers (connected via the telecommunication line)

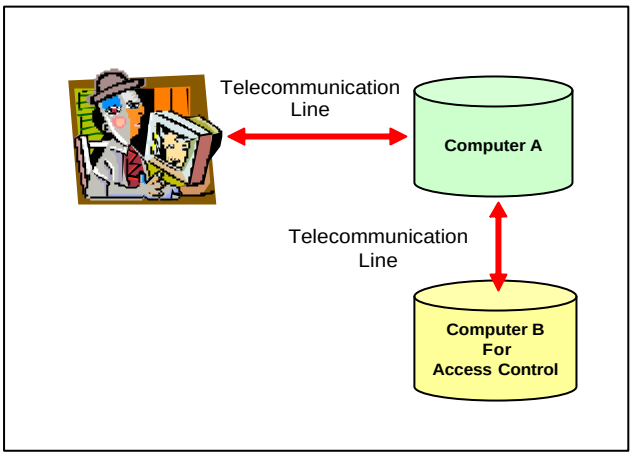


Fig. 5: unauthorized computer access in Article 3 Paragraph 2 (3)

These mentioned above are all "unauthorized computer accesses" that shall be punished by Article 8 of this law. Despite the enactment of this law, many unauthorized computer accesses have been taking place every year. Target computer systems are the Web Server, e-mail Server, mobile phone Server and so on. In fact there are many unauthorized computer accesses in Japan, but only a few court cases are published [See Case 5]. The number of unauthorized computer accesses is released by the Japan Police Agency [Table 6][31].

Year	2002	2001	2000
The number of arrested people	51	35	31

Table 6: the number of unauthorized computer accesses

[Case 5]
Free-mail Server Unauthorized Access Case (16 October 2002, judgment, case number; Heisei 14 WA Criminal 62 etc., Takamatsu District Court Marugame Branch)32

(FACTS)
The accused accessed e-mail server by using speculated ID and password of a woman without any permission, and he sent some e-mails by means of the woman's e-mail account. After that, he had deeply interested in a secret sexual party which was managed via e-mails. He accessed the e-mail server of the party e-mail by similar means. Also he obtains some secret which were sent and received at the secret party.

(COUNTS)
Article 8 and 3 of Unauthorized Computer Access Law – Unauthorized Access
Article 104 of Telecommunication Business Law33 - violation of the secrecy of communications

[30] If the target computer is Computer B then Article 3 Paragraph (2) can be applicable, because an access control function is installed in the Computer B itself.
[31] See also Table 2.
[32] This case can be found only at the Web Site of Supreme Court of Japan (in Japanese).
[33] Article 104 provides as follows;
(1) Any person who violates the secrecy of communications being handled by a telecommunications carrier (including communications stipulated in the provisions of Article 90 paragraph (2)) shall be guilty of an offense and liable to penal servitude for a term not exceeding one year or to a fine not exceeding three hundred thousand yen.
(2) Any person who engages in the telecommunications business and commits the act referred to in the preceding paragraph shall be guilty of an offense and liable to penal servitude for a term not exceeding two years or to a fine not exceeding five hundred thousand yen.
(3) An attempted offense of the preceding two paragraphs shall be punished.

(JUDGMENT)
Takamatsu District Court Marugame Branch concluded guilty on all his counts and ordered the accused to be one year penal servitude (imprisonment with compulsory labor) with three years suspension of execution.

Also this law prohibits the following activities relating to unauthorized access. These activities can involve teaching another person's access ID, password and other identification measures.

Article 4 Prohibition of acts of facilitating unauthorized computer access
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.

In addition, The Metropolitan Public Safety Commission and Prefectural Public Safety Commission shall provide advice and guidance for the purpose of preventing a recurrence of similar acts. And a person who has engaged in the relevant work to this assistance shall not reveal secret information he or she has learned.

Article 6 Assistance, etc., by Metropolitan and Prefectural Public Safety Commissions
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 the following activities shall be punished under Article 8 and 9 of this law. Article 8 (1) is the punishment for unauthorized accessing, Article 8 (2) is the punishment for facilitating unauthorized computer access and Article 9 is the punishment for revealing secret information.

Article 8 Penal provisions
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)

Problems on what is "illegal access"

The requirements of "unauthorized access" in this law are mentioned above. The scope of protected computer system is limited to "a specific computer". "A specific computer" means a computer system connected with another computer system via telecommunication line. And only accessing via telecommunication line shall be punished by this law. In addition, "a specific computer" have had added any access control function [See Fig. 3]. Thus the 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, even if such computer system is connected with other computer system via telecommunication line)
3) Any access to any computer systems to which any access control function has not been added

By the way, the Cybercrime Convention (ETS 185) has the following definition provision (Article 1) and substantive criminal law provision (Article 2). "Illegal access" shall be punished by domestic law. In general, many scholars of criminal law believe that an illegal access is the same as an unauthorized access.

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 this definition in the Cybercrime Convention, 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 and that these 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 the fact that most business companies have urged that such non-remote unauthorized access also shall be punished by law[34].

On this problem, many business companies believe and urge that any unauthorized access to the stand alone computer system also shall be punished by law[35]. Nevertheless, the Minister of MOJ didn't consult with the Advisory Committee on this problem on March 2003.

Other Cybercrimes

Digital Pornography and Child Pornography

In Japan, there are two laws relating to 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).

[34] 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.
[35] Research Report by the Cybercrime Study Group at the Ministry of Economy, Trade and Industry (2001, in Japanese)
http://www.meti.go.jp/kohosys/press/0002626/1/020418cyber.pdf

Distribution of obscenities

The penal Code of Japan prohibits any distribution of obscenities.

Article 175 Distribution of obscenities
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 was 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 [Case 6] of Japan decided an opposite result that any hard disk drives which have any pornographic data stored in shall be deemed as obscenities. Many scholars have different opinions to the Supreme Court's judgment.

On March 2003, the Minister of MOJ consulted also this problem to the Advisory Committee. Article 175 will be amended so as to include digital pornographies.

[Case 6]
FL Mask Case (July 16 2001, judgment, case no.; Heisei 11 A 1221, Supreme Court) 36

FL Mask is a randomize software to protect any computer data. In this case, FL Mask was used for randomizing many pornography data. The Supreme Court dismissed the final appeal.

(ARGUMENTS)

Decision concerning the case where obscene image data is stored on the so-called PC Net host computer for an unspecific number of people to reproduce and concerning whether it constitutes a display of obscene object in pubic or not

(JUDGMENT)

1. A hard disc of the so-called PC Net host computer containing and storing obscene image data is obscene objects set forth in Article 175 of the Penal Code.
2. "To display in public" obscene objects under Article 175 of the Penal Code means to put the obscene contents thereof in a state for an unspecific number or a large number of people to recognize, and for the purpose of the definition, it is not required to create the state for people to recognize obscene contents easily without taking special actions.
3. To store and keep obscene image data on a hard disc of the so-called PC Net host computer so that an unspecific number of service subscribers can download the said image data by means of their own PCs and put the said image for reproducing/viewing by means of a image display software constitutes "to display in public" obscene objects under Article 175 of the Penal Code.

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 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

[36] This case can be retrieved at the Web Site of the Supreme Court (footnote 5).

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 the Ministry of Justice)37

Also in Japan, many crimes relating to child pornography have been taking place continuously. The number of child pornography crimes is released by the Japan Police Agency [Table 7][38].

Year	2002	2001	2000
The number of arrested people	140	128	113

Table 7: the number of child pornography crimes

There are many court rulings. However, sometimes these court rulings contradict 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 prohibit 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 be protected and given a good education. In the National Diet of Japan, an amendment bill of this law is now proposed due to those problems and discussions.

Copyright Infringement

Any infringement of digital copyright shall be punished by the Copyright Law of Japan. This Copyright Law has been addressed to the Cybercrime Convention completely. And there are many court cases both civil and criminal relating to the copyright infringement.

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 ownership 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

[37] This translation can be found at the Web Site of MOJ.
http://www.moj.go.jp/ENGLISH/CRAB/law01.html
[38] See also Table 2.

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 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))[39]

Perspectives

On 24 March 2003, the Minister of MOJ consulted a legislative examination with the Advisory Committee on the Legal System in the Ministry. This consultation is based on the conception of the "Harmonization of Criminal Law in the field of Cybercrime"[40] and includes the following subjects;

1) Ban on illegal computer programs (Computer virus, Hacking tools etc.)
2) Ban on digital pornography (amendment of Article 175 of the Penal Code)

[39] This translation by CRIC can be found at the Web Site of CRIC. http://www.cric.or.jp/cric_e/clj/clj.html
[40] See Cristian Swarzenegger, *Die internationale Harmonisierung des Computer- und Internetstrafrechts durch die Convention on Cybercrime vom 23. November 2001 – Am Beispiel des Hackings, der unrechtmassigen Datenbeshaffung und der Verletzung des Fernmeldegeheimnisses (Ersheinungsdatum: 26. Juni 2002)*, Andreas Donatsh, Marc Forster, Cristian Schwarzenegger (eds.): Strafrecht, Strafprozessrecht und Menshenheit – Festschrifft für Stefan Trechsel zum 65. Geburttag, Zürich: Schlthess, 2002, pp.305-324.

3) Establishment of proceedings on search and seizure of a computer data
4) Establishment of confiscation of computer data

As my private perspectives on future Cybercrime legislation, I would like to explain the aims of this consultation and the possibility of enactment based on these consulted matters. Also I would like to point out some additional problems relating to the future legislation and law enforcement.

Illegal computer programs

The aim of this subject by the consultation is to address Article 6 of the Cybercrime Convention (ETS 185) on a misuse of devices.

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.

This Article defines "device" as a device that is designed or adapted primarily for the purpose of committing any computer crimes, and a computer program is also included in the device. However the consultation from the Minister of MOJ is related only to a production, a distribution, an execution, an obtention and a possession of an illegal computer program. The illegal computer program may involve various malicious computer programs, for instance a computer virus, Worm program, Hacking program and Spy software.

The production of computer virus program itself can not be punished by the current laws. If any destructive results are caused by the computer virus programs then relevant laws shall be applied. For instance, such activities may be punished by Article 258 or 259 of the Penal Code as the destructions of electromagnetic record. Of course, if the distribution of computer virus programs causes a obstruction of business then relevant penal laws are applicable [41] So there is no such provision as a ban on the illegal computer program production in the current laws. And most computer viruses can be blocked by means of technological measures, for instance by anti-virus software and other similar devices.

However in fact, no one can stop the productions of new type computer viruses and other similar malicious computer programs. So there is a necessity of the enactment of the law to ban on the production of such malicious computer programs.

By the way, some people come out against such legislation. The main reason of opposition is that the difference between the illegal computer program and legitimate security tools is not so clear. In fact in many cases, the same computer program can be used both for Hacking and for a security. However, as mentioned in Article 6 Paragraph 2 of the Cybercrime Convention, a ban on the illegal computer program requires the existence of the purpose of committing an offence established in accordance with Articles 2

[41] We can discover only one court case on a computer virus in Japan. In this case, a boy was accused under Article 234 of the Penal Code (Obstruction of business by influence). However, the court ruling of this case is not published, due to that this case is a juvenile case.

through 5 of this Convention. Probably future Bill on the basis of this consultation will have such a limitation.

Digital pornography

On this point, I already discussed in the section on Article 175 of the Penal Code. The major interpretation by courts on Article 175 of the Penal Code has been wrong. Only a few people are opposed to an enactment of a ban on digital pornography. Only one problem is that current Article 175 of the Penal Code covers only tangible pornography originally. So in accordance with the conception of "Nullum poena sine lege - Nullum crimen sine lege (Without a law, there is no punishment. Without a law, there is no crime.)", Article 175 of the Penal Code shall be amended.

Search and seizure of a computer data

Evidence that has an electronic form is not tangible evidence. Despite this most important evidence related to computer crimes is an electronic data: the current criminal procedure law is constructed only on the basis of tangible real world. So the Cybercrime Convention Article 19 provides as follows;

Article 19 – Search and seizure of stored computer data (ETS 185)
1 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to search or similarly access:
a a computer system or part of it and computer data stored therein; and
b a computer-data storage medium in which computer data may be stored
in its territory.
2 Each Party shall adopt such legislative and other measures as may be necessary to ensure that where its authorities search or similarly access a specific computer system or part of it, pursuant to paragraph 1.a, and have grounds to believe that the data sought is stored in another computer system or part of it in its territory, and such data is lawfully accessible from or available to the initial system, the authorities shall be able to expeditiously extend the search or similar accessing to the other system.
3 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to seize or similarly secure computer data accessed according to paragraphs 1 or 2. These measures shall include the power to:
a seize or similarly secure a computer system or part of it or a computer-data storage medium;
b make and retain a copy of those computer data;
c maintain the integrity of the relevant stored computer data;
d render inaccessible or remove those computer data in the accessed computer system.
4 Each Party shall adopt such legislative and other measures as may be necessary to empower its competent authorities to order any person who has knowledge about the functioning of the computer system or measures applied to protect the computer data therein to provide, as is reasonable, the necessary information, to enable the undertaking of the measures referred to in paragraphs 1 and 2.
5 The powers and procedures referred to in this article shall be subject to Articles 14 and 15.

The consultation by the Minister of MOJ is similar to this Article 19 of the Cybercrime Convention. To establish the reasonable proceedings to search or seize electronic evidence is itself a very important and necessary matter. However at the same time, especially to avoid over seizure, the new proceeding has to be established. If the relevant provisions in the criminal procedure law and the enforcement policy of the law are not so clear then the interpretation of them become arbitrary and the border of the law enforcement power would be vague too. A revoked case relating to the distribution of digital obscenities may suggest this [Case 7][42].

[Case 7]
Bekkoame Case (18 February 1998, decision, case number; Heisei 10 MU Criminal 141, Tokyo District Court)43

(FACTS)

[42] Similar problems are taking place all over the world. And many human rights groups are skeptical about the legitimacy of law enforcement officer's activities. They fear that the existing law enforcement powers especially on surveillance will be extended. For example, the Privacy International points out the fact of over collections of customers data by UK police officers.
http://www.privacyinternational.org/countries/uk/surveillance/knowdatacampaign.html
[43] Hanrei-Jiho no.1637 p.152

Bekkoame was one of the most famous Internet Service Provider as "the Cathedral of pornography" at the time. In 10 February 1998, police officers of Fukuoka Prefecture Police Office seized many pornography data and related document at the office building of Bekkoame in Tokyo. This search and seizure was based on the search and seizure order issued by a judge of the Fukuoka Summary Court. Many paper documents were involved in such seized materials including customer lists of Bekko-ame. Bekkoame was not the suspect, and the handle name of the suspect at the Bekko-ame Site was already specified by the police officers. So Bekkoame filed a protest against this seizure proceeding.

(CLAIMS)

Revoke the seizure of customer lists etc.

(SUSPECTED CRIME)

Article 175 - distribution of obscenities

(DECISION)

Tokyo District Court evoked the seizure of customer lists. But, the rest claims by Bekko-ame were all dismissed.

(COURT OPINION)

The search and seizure order indicates "server computers, disk alleys, rooters and related telecommunication devices, flexible disks and other electromagnetic medias on which suspected data are stored, personal computers, hard disk units and similar boot devices, printers, notes and files relating to complaints from customers, advertisement materials on BBS service, documents relating to advertisement, account books, receipts on service charges, vouchers, subscription documents, customers lists, e-mail messages, backup copies of e-mail messages, private telephone number lists, postal address lists, pocketbooks and similar papers, name cards, ID number registration papers, passbooks, seals" as the goods to be seized.

However, to execute the search and seizure order legitimately, seized goods have to be limited within the extent necessarily to get the best evidence to prove the suspected crimes. In this case, there is no evidence to prove the necessity for the seizure of the customer lists. Such seizure is out of relevant laws.
The seizure of customers list shall be revoked. Because the customer lists involve the information of another customers with the exception of the suspected person and such lists are not necessary to this criminal investigation.

I believe that the amendment of the criminal procedure law based on the consultation be the Minister of MOJ itself is reasonable. But many service providers are anxious about the corporation duty as indicated at Article 19 Paragraph 4 of the Cybercrime Convention. On the other hand, there is other merit for the service providers that they can continue to provide their service to their users at the time of search or seizure. If new proceedings will not be established, then hard disk drives in their Server can be removed as evidence by the law enforcement officers.

This is a very difficult problem, but the amendment of the current criminal procedure law on this point will be done successfully.[44]

Confiscation of a computer data

Current confiscation procedure is based only on tangible goods. The consultation related to this point is clearly right. Article 19 of the Penal Code provides as follows;

Article 19 confiscation
The following things may be confiscated;
(1) Things having constituted a criminal act;
(2) Things used or intended for use in a criminal act;
(3) Things resulting from or acquired by a criminal act or those acquired as compensation for a criminal act;
(4) Things acquired in exchange for those mentioned in the preceding item.
2 Confiscation may be enforced only if the object to be confiscated belongs to a criminal. Provided that, when a person other than a criminal, being aware of the object as such, has acquired it after the commission of a crime, the object may be confiscated even though it belongs to the person.

[44] There are some different problems relating to the court proceedings. In ordinary cases, electronic evidence might be permitted as legitimate evidence only when the print outs of such electronic evidence brought into the court. In many cases, there is no equipment for examining such electronic evidence directly. So if new search and seizure proceedings are introduced by the amendment of the criminal procedure law, then the courts of Japan would have to address such fundamental changes in the area of evidence.
On electronic evidence, See Alan M. Gahtan, *Electronic Evidence*, Carswell, 1999

(Translation by Ex-Professor Fukuo Nakane)

In accordance with a general interpretation, “Things” in Article 19 means only tangible goods. And an electronic data is not a tangible good. In many case, Hard Disk Drive on which illegal data stored have been searched, seized and confiscated. However, at the same time, another person’s data also have been searched, seized and confiscated together with suspected electronic data. At the worst, all data stored in such Hard Disk Drives would be deleted or broken through the confiscation proceedings. So it is very important to establish the clear proceeding that only the data of the accused can be deleted as a confiscation.

Perspectives on Cyber legislation

This consultation by the Minister of MOJ may be reasonable and has a sort of necessity. Possibly, the Committee will receive an agreement to the consultation and draft the amendment bill. This bill will include the Penal Code amendment part and the criminal procedure law amendment part.

However, if the amendment bill will be enacted then some of these problems can be resolved by the new law, but at the same time other problems may take place.

For instance, the courts of Japan have to prepare necessary equipment and skills to address the new electronic evidence. Practicing lawyers and the prosecutors also have to study new crimes and proceedings. But, these may be a pure practical issue.

On the other hand, theoretical problems also remain. Especially it would be a bit funny that the consultation by the Minister of MOJ doesn’t include a ban on illegal interception of communication and a ban on an unauthorized computer access to a stand alone computer. These matters will be discussed continuously also in future. At the same time, such theoretical problems are located in the area of policy making to address cybercrimes.

Conclusions

There are many fundamental cybercrime laws in Japan. However, some important omissions can be found in Japanese legislations, especially in relation to the Cybercrime Convention, where many problems remain. Also some confusions and contradictions can be found in Japanese court cases. Thus more studies and examinations relating to the existing laws and international instruments on cybercrimes have to be done.

In his Remarks at the FTC SPAM Forum 2003[45], Commissioner Mr. Orson Swindle mentioned “This is a journey, not a destination.” I agree with his opinion absolutely. We have to examine more and more, we are sharing same problems caused by Cybercrimes.

Further, I believe that more clear legislation policy has to be established, especially relating to cyber legislation. Ambiguousness would bring confusions and contradictions to the sphere of law enforcement. In addition such a legislation policy should be harmonized with an international consensus.

[45] This conference was held on 30th of April – 2nd of May 2003 in Washington DC. I was presented at this conference.
http://www.ftc.gov/bcp/workshops/spam/