ALAI 2001 National Report
Session IC
Japan

Prepared by Mr. Kentaro ENDO and Prof. Hiroshi SAITO.

1. Types of Circumvention

Some intention or result of circumvention could lead to crime in the Copyright Law or the Criminal Law.

a. Yes. For example, the Unauthorized Computer Access Law prohibits such acts.

<The Unauthorized Computer Access Law>

(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 putting into 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 putting into 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 putting into 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.

b. Yes. For example, the Broadcast Law prohibits such acts.

<The Broadcast Law>

Article 52-5. Any person shall not, unless having concluded an agreement with a paid broadcaster for receiving the paid broadcasting services from the latter on the basis of approval agreement clauses etc., receive said paid broadcasting with the use of receiving equipment for said paid broadcasting in Japan.

c. Yes. For example, the Unauthorized Computer Access Law prohibits such acts.

d. A person could be liable for having engaged in such an act under the general tort law rule.

e. A person could be liable for having engaged in such an act under the general tort law rule.

f. Yes. For example, the Copyright Law prohibits such acts.

<The Copyright Law>

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

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

g. A person could be liable for having engaged in such an act under the general tort law rule.

h. A person could be liable for having engaged in such an act under the general tort law rule.

2. General tort rules of direct or secondary liability

a. Yes, he/she could be liable. / Concerning technological protection measures, 1) in spite of foreseeing or being able to foresee obviously circumvents of contents receiver with a view to not paying adequate compensation, 2) to offer a device or a program having a function for the circumvention of technological protection measures, 3) and infringe on the business interests of another person, generally forms tort.

b. We are not aware of such a case.

c. –

d. It might be considered an "abuse of right" when it is the exercise of right having intention of offense.

3. Broadcasting law, cable and satellite regulations, protection of encrypted services or broadcasts, protection of conditional access services

a. Yes. (the Broadcast Law and the Copyright Law) / The public purpose for this prohibition is for example, conservation of management bases of paid broadcasting.

<The Broadcast Law>

Article 52-5. Any person shall not, unless having concluded an agreement with a paid broadcaster for receiving the paid broadcasting services from the latter on the basis of approval agreement clauses etc., receive said paid broadcasting with the use of receiving equipment for said paid broadcasting in Japan.

b. Yes. (the Copyright Law) / To make sound or visual recordings of their broadcasts or those diffused by wire from such broadcasts, and to reproduce by means of photography or other similar processes the sounds or images incorporated in these broadcasts without authorization is prohibited.

c. Yes. (the Copyright Law) / A device having a principal function for the circumvention of technological protection measures is illicit. / No / Distribution, lending, manufacture, import and possession / A device having a "principal" function for the circumvention of technological protection measures is illicit. / Copyright holders etc. / Criminal penalty

Yes. (the Unfair Competition Prevention Law) / Sales and related activities for devices and programs that circumvent technological measures to control use or copying of contents are classified as "unfair competition". / Sales and related activities are not prohibited but classified as "unfair competition". / Nothing / Content providers (content delivery companies, and manufacturers of devices, etc.) / Injunction requests and compensation requests for damages

<The Copyright Law>

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

d. Probably no.

e. No comment

f. 1. No

2. –

3. –

4. Telecommunications Law

a. Yes.

1. Interception and disclosure / No.

2. No.

3. Nothing

4. Telecommunication organizations etc. / Compensation requests for damages

b. Mandatory technical standards in the Radio Law etc. probably could not lead to prohibiting devices enabling the unauthorized reception of communications.

5. Computer crime

a. Yes. (the Unauthorized Computer Access Law) / Yes. / 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

b. See below.

<The Unauthorized Computer Access Law>

(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 putting into 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 putting into 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 putting into 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.

(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.

c. No. / No. / See below.

<The Unauthorized Computer Access 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.

<The Unauthorized Computer Access Law>

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.

d. No.

e. No.

f. We are not aware of such cases.

6. Unfair Competition law or unfair commercial practices

a. Yes / Sales and related activities for devices and programs that circumvent technological measures to control use or copying of contents are classified as "unfair competition" under the Unfair Competition Prevention Law.

b. Advantage: Injunction request is possible.

Disadvantage: Those who have cause of action are limited.

7. Protection of technological measures as such

a. Nothing

b. –

8. Other protections

a. We are not aware of any other means.

b. 1. We do not know.

2. We do not know.

9. Limitations, exception, fundamental rights, third parties' and public interest

a. Privacy of communications might be applied.

b. We do not know.

10. Potential application of the protections surveyed in Questions 1-9 to copyrighted works

a. Yes. / It depends on the nature of copyright holders in each case.

b. Yes.

c. – (Copyright-specific protection was established.)

d. – (Japan acceded to the WIPO Copyright Treaty in 2000.)