sometimes, the family court must hear the statements of children even below this age in the light of the interests of children.

4. Criminal Law and Procedure

The Act on the Partial Revision of the Act on the Prohibition of Unauthorized Computer Access, etc.
Law No. 12, March 31, 2012 (Effective on May 1, 2012).

Background:

In 1999, the Act on the Prohibition of Unauthorized Computer Access, etc. (Law No. 128 of 1999) was established. In this act, unauthorized computer access is prohibited, and once unauthorized computer access has been gained, this lawbreaking can be punished as a cybercrime, which had been limited previously to the acts that do actual harm, such as computer fraud and obstruction of business by destroying a computer, before this act was established. Furthermore, in order to strengthen measures against cybercrime, the obligation to endeavor to take these measures is imposed on the access administrator and the prefectural public safety commissions and national government are obligated to back up the access administrator and others in this act.

For the past dozen years or so after the establishment of this act, the domestic situation surrounding the advanced information and communications network society has changed. First, the Internet has become popular as an infrastructure to support the basis of Japanese society and economy. Second, since the effectuation of this act in 2000, both the numbers of cleared cases and persons for the crime of unauthorized computer access have been on the increase, and serious cybercrimes have frequently occurred. Third, there have been many cases of cybercrimes through use of phishing. Phishing scams are to get a holder of the right of access to type in his/her ID and password and to defraud this holder of his/her ID and password, typically, by masquerading as an actual access administrator, and launching a phishing website or sending a phishing e-mail to that holder. Fourth, the incidence

of unauthorized login attempts by continuous automatic input programs was recognized by police organization. Fifth, the measures which access administrators have taken against cybercrime have been inadequate. From these five different standpoints, we can recognize the change of the domestic situation surrounding the advanced information and communications network society and the necessity of an amendment to the Act on the Prohibition of Unauthorized Computer Access, etc. of 1999. Therefore, this act was partially revised in order to respond to that situation and ensure the effectiveness of the prohibition against unauthorized computer access.

Main Provisions:

1. Prevention of the Illegal Distribution of Identification Codes
   (1) Prohibition and Punishment of the Unauthorized Acquisition and Retainment of Another Person's Identification Code
   In the Act on the Partial Revision of the Act on the Prohibition of Unauthorized Computer Access, etc. of 2012, the unauthorized acquisition and retainment of another person's identification code for access control for the purpose of use for the commission of unauthorized computer access are prohibited (the revised Act on the Prohibition of Unauthorized Computer Access, etc., Articles 4 and 6).
   Any person who has perpetrated such acquisition or retainment shall be imprisoned with labor for a maximum term of one year, or imposed with a fine of up to five hundred thousand yen (Article 12, Items 1 and 3).
   (2) Stepping Up Prohibition and Punishment of the Provision of Another Person's Identification Code
   In the said Act, the provision of another person's identification code for access control for any person other than an access administrator who is involved with this access control and a holder of the right of access who is authorized to use that identification code is prohibited, unless there is some justifiable reason (Article 5). Through the partial revision in 2012, the requirement that it is clear in which website another person's identification code in question can be utilized was deleted from this article.

Any person who has perpetrated such an act shall be imposed with a fine of up to three hundred thousand yen (Article 13). In addition, any person who has perpetrated such an act, while knowing that the recipient of another person's identification code has a purpose to use it for the commission of unauthorized computer access, shall be imprisoned with labor for a maximum term of one year, or imposed with a fine of up to five hundred thousand yen (Article 12, Item 2).

(3) Prohibition and Punishment of Phishing

In the said Act, causing a perpetrator to be mistaken for an actual access administrator, such as pretending to be this administrator, and both launching the website which requests a holder of the right of access to type in his/her identification code for access control and sending this holder the e-mail which does the same are prohibited, unless that administrator accepts (Article 7).

Any person who has perpetrated a phishing like that shall be imprisoned with labor for a maximum term of one year, or imposed with a fine of up to five hundred thousand yen (Article 12, Items 4).

2. Raise of Statutory Penalty in the Penal Provision Pertaining to Unauthorized Computer Access

In the said Act, the statutory penalty for unauthorized computer access was raised from an imprisonment with labor for a maximum term of one year or a fine of up to five hundred thousand yen, to three years or one million yen (Article 11).

3. Enlightenment and Dissemination of Knowledge by the Prefectural Public Safety Commissions

In the said Act, the prefectural public safety commissions are required to enlighten people and disseminate knowledge in regard to the protection against unauthorized computer access (Article 9, Paragraph 5).

4. Aid to Organizations that Support the Measures which Access Administrators have taken against Cybercrime

In the said Act, the National Public Safety Commission, Minister of Internal Affairs and Communications, and Minister of Economy, Trade and Industry are required to back up (e.g. provide necessary information to) organizations that support the measures which access administrators have taken against cybercrime (Article 10, Paragraph 2).

Editorial Note:

The advanced information and communications networks, such as the Internet, have improved convenience in national life and served as an infrastructure to support the basis of Japanese society and economy. On the other hand, cybercrimes have become more serious. For instance, unauthorized computer access with regard to the Internet banking occurred frequently in 2011. According to the National Police Agency, between March and December of 2011, 165 accounts of 56 financial institutions in 35 of 47 prefectures in Japan suffered damage from unauthorized computer access, for which identification codes for access control appear to have been obtained through use of phishing or malicious program. As a result, the total sum of money illegally remitted by that unauthorized computer access amounted to about three hundred million yen. In this way, the situation concerning the violation of the law banning unauthorized computer access has not been sufficiently ameliorated. Therefore, we expect the effective operation of the said Act.

5. Commercial Law

Adoption of the "Outline Proposal for the Review of Company Law" on September 7, 2012

Background:

The Company Law Subcommittee of the Legislative Council compiled the "Outline Proposal for the Review of Company Law" on August 1, 2012, and it was adopted by the General Assembly of the Legislative Council on September 7, 2012. The Company Law Subcommittee was launched on February 24, 2010 in response to the advisory by the Minister of Justice. After the adoption of the Outline Proposal, a general election of the House of Representatives was held on December 2012, and the change of government from the Democratic Party of Japan, which had lasted three years and three months, to the Liberal Democratic Party occurred. Perhaps because of the effects of the change of government, the