Section 3
Establishment of a Safe and Secure Ubiquitous Network Society

1. Consumer administration in relation to telecommunications services

(1) Illegal and harmful information on the Internet

A. Dealing with illegal/harmful materials on the Internet

The Internet has penetrated Japan at a remarkable pace and has been used as a form of social infrastructure, serving as an indispensable part of people's lives. At the same time, the rapid penetration of the Internet has also generated negative effects, such as the transmission of illegal and harmful information. The Ministry of Internal Affairs and Communications (MIC) established the Study Group to Address Illegal and Harmful Information on the Internet in November 2007 to examine comprehensive actions to deal with illegal and harmful information, including further promotion of installation of filtering software to protect children and released a final report in January 2009.

B. Establishment of the Law Concerning Environment for Children to Safely Use the Internet

At the 169th Diet session, the Law Concerning Environment for Children to Safely Use the Internet (hereinafter referred to as the Law on Internet Environment for Children) was initiated by lawmakers and enforced in April 1, 2009. The law focuses on measures to protect minors (those under 18 years of age) from harmful information and explicitly provides for the direction of future efforts with respect to a vision of the environment for Internet utilization.

C. Promotion of filtering

Today, we are seeing a number of cases where young people access harmful Internet sites, such as so-called online dating sites and get involved in crime, which is becoming a social problem. With the development of the Law on the Internet Environment for Children in June 2008, the following measures have been taken since April 1, 2009: Mobile phone business operators shall in principle be obliged to set up filtering functions before selling minors (those under the age of 18) mobile phones that can be used to access the Internet; providers shall be obliged to provide filtering functions when requested by users; and manufacturers of equipment that can be used to access the Internet, such as personal computers, shall be obliged to take measures to facilitate the use of filtering functions before selling the equipment. Also, guardians and parents shall be responsible for the appropriate supervision of Internet use by minors under their protection.

D. Formulation of a program to promote the creation of a safe network

In response to the establishment of the Law on Internet Environment for Children and the revised Law on Regulation of Transmission of Specified Electronic Mail at the 169th Diet session, the MIC formulated a program to promote the creation of a safe network and protect the ministry against illegal/harmful information in January 2009. This program is a comprehensive policy package with the three pillars: (1) development of basic framework that provides a sense of safety, (2) promotion of voluntary efforts by the private sector and (3) promotion of efforts to educate users.

E. Formulation/revision of the guidelines related to the Provider Liability Limitation Law

The Provider Liability Limitation Law was enforced in May 2002 as a measure against increasing cases of information violation of the rights of others on a website or BBS, etc. This law provides (1) limitation/clarification of damage liability of providers in cases where the rights of others are violated and (2) the rights of a person whose rights have been violated to demand the provider to disclose the information source. So as to ensure the stringent enforcement of the law, the MIC supports and provides information about the Council for the Guidelines for the Provider Liability Limitation Law, which comprises business associations and right holders' associations.

F. Support for voluntary response of providers to illegal/harmful information on the Internet

The MIC, together with four organizations associated with the Telecommunications Carriers Association, examined the measures for promoting appropriate and prompt responses of providers to illegal information and information that may offend public order and morals on the Internet, and formulated Guidelines concerning Responses to Illegal Information on the Internet and the Model Conditions of Contract concerning the Responses to Illegal/Harmful Information in November 2006. In response to newly emerging problems such as "dark

sites" or the transmission of information on committing suicide using hydrogen sulfide, the above-mentioned guidelines and the model conditions were revised in December 2008. Also in January 2008, the Consultation Center for Illegal/Harmful Information Business was established within the Telecommunications Services Association to offer advice and consultation pertaining to illegal/harmful information for business operators, such as providers.

(2) Measures against nuisance e-mails/ phishing

A. Measures against nuisance e-mails

The MIC established the Study Group to Examine Comprehensive Ways to Deal with Nuisance e-Mails in July 2007, and the interim report of the study group was released in December 2007 and the final report in August 2008.

The interim report made recommendations on the revision of the Law on Specified Electronic Mails. Based on the recommendations, the law was revised to include regulations against nuisance e-mails by the opt-in method and was developed in June 2008 and enforced on December 1, 2008.

The final report includes recommendations on the following matters: (1) framework of comprehensive measures against nuisance e-mails, (2) operation and enforcement of laws and regulations by the opt-in method, (3) technological measures, (4) voluntary measures by telecommunications business operators, (5) improvement of PR campaigns and consultation for users, (6) promotion of international collaboration and (7) system for comprehensive measures against nuisance e-mails. Based on these recommendations, the MIC formulated and released the Guidelines concerning Sending Specified Electronic Mails in November 2008.

B. Measures against phishing

Phishing is illegally obtaining personal information such as addresses, names and bank account numbers by sending an e-mail in the guise of a person with credibility, such as a financial institution, and inducing the recipient to access a false website. Sending an e-mail is one of the main ways of luring users to a phishing site. Since the amended Law on Specified Electronic Mails includes a provision whereby telecommunications operators can refuse the provision of service if a sender sends e-mails from a false e-mail address, it can also be an effective countermeasure against phishing.

(3) Safe and secure use of mobile phones

A. Appropriate enforcement and revision of the Law on Prevention of Abusive Use of Cellular Phones

The Law on Identification of Cellular Phone Users by Mobile Operators and Prevention of Abusive Use of Cellular Phones (hereinafter referred to as the Law on Prevention of Abusive Use of Cellular Phones) stipulates the following with regard to countermeasures against the illegal use of cellular phones, such as billing fraud: (1) mobile phone business operators shall be obliged to identify the contractor at the time of concluding a contract or transfer (2) the police chief unit may demand that the mobile phone business operator verify the contractor if a phone is suspected of being used for a crime, (3) renting (with charge) a mobile phone without confirming the name and address of a client and unauthorized transfer of a mobile phone shall be strictly prohibited. The MIC is committed to appropriately enforce the amended law, and two correction orders were issued in FY2008.

In recent years, since cases have emerged where the existing regulations cannot strictly control crimes, such as an increase in cases of rental mobile phones being used for crimes like billing fraud, the said law was partially amended in June 2008 and put into effect on December 1, 2008, together with the revised ordinances. The amended law stipulates that (1) mobile phone business operators shall be obliged to make the confirmation of the customer's identity more imperative at the time of concluding a rental contract and to keep identity verification records in a safe place, (2) the unauthorized transfer of a SIM card shall be subject to penalty and (3) the government shall provide information and take measures to heighten public awareness.

(4) Protection of personal information in the telecommunications field

A. Formulation/revision of Guidelines concerning Protection of Personal Information by Telecommunications Business Operators

In 1991, the MIC formulated and enforced the Guidelines concerning Protection of Personal Information by Telecommunications Business Operators in order to protect personal information in the area of telecommunications business. Then, the MIC conducted discussions based on the establishment of the Personal Information Protection Law and full-fledged revisions and additional interpretations were added to the guidelines in August 2004. In October 2005, additional provisions and revised interpretations were made based on the Specified Electronic Mails Law. In September 2007, the interpretation of the guidelines was partially revised in response to the diversification of positioning informa-

tion services and penetration of terminals with GPS functions.

B. Formulation/revision of the Guidelines concerning Protection of Personal Information of Broadcast Receivers

The MIC formulated the Guidelines concerning the Protection of Personal Information of Broadcast Receivers in August 2006 after the fully-fledged enforcement of the Private Information Protection Law in April 2005. These guidelines were reviewed in July 2007 in line with the changes that occurred after the enforcement, and were partially revised with respect to the following two points: (1) clarifying who may acquire personal information of viewers, etc., and (2) safe handling of the personal information recorded on a reception device.

2. Promotion of information security policy

(1) Information security measures of the government

Japan's efforts for information security issues have been enhanced, with the setting up of the National Information Security Centre (NISC) in the Cabinet Office in April 2005 and the establishment of the Information Security Council in the IT Strategy Headquarters in May 2005.

In February 2006, the Information Security Council developed the First National Strategy on Information Security, which is a medium- and long-term strategy covering the three years from 2006 to 2008, and in February 2009, the Second National Strategy on Information Security covering the three years from 2009 to 2011. Also, based on this plan, Secure Japan 2009 was finalized in June 2009.

(2) Realization of an environment for safe and secure use of the Internet

Based on the u-Japan policy and the Second Information Security Basic Plan, etc., the MIC has been making efforts toward responding to diversified products and the improvement of human and organizational capacities that would lead to the enhancement and increased reliability of networks which, from the standpoint of a competent ministry in the ICT field, is one of the most important infrastructures, in order to develop an environment where people can use information and communications networks safely.

(3) Ensuring safety and reliability in the telecommunications services

As IP telephony networks advance and the use of various new IP-related services expands, IP service-related communications interferences have been occurring more frequently, and they are also larger in scale and longer in duration.

In order to respond to these changes, deliberations have been conducted at the Information and Communications Council, and the MIC received a partial report titled Safety/Reliability Measures for IP Based Networks in May 2007 and Safety and Reliability Standards for IP Based Networks in January 2008 from the council. Based on these, the MIC set up the IT Network Management Human Resources Study Group in April 2008 with the aim of collecting opinions and views on the system management of the network with advancing IP and related human resources activities, and the final report was prepared and announced in February 2009. The report examined the skills of chief telecommunications engineers responding to the advancement of IP and reviewed the certification exam for chief telecommunications engineers.

3. Ensuring reliability of electronic data

In order to promote socio-economic activities further, using a network such as e-commerce and ensuring a smooth user environment for electronic signatures attached to electronic data, the Law concerning Electronic Signature and Certification Services has been enforced since April 2001 in Japan. As of the end of April 2009, 18 specific certification services have been accredited.

The "time business" (a collective term for the Time Authority and Time Stamp Authority) is becoming increasingly important. This includes time stamps attached to electronic data that would improve reliability at the time of creating electronic data that is distributed and stored in the field of e-commerce and associated services. The MIC has been actively making efforts to promote the use of time business by formulating and releasing the Guidelines concerning Time Business in November 2004.