Section 3
Establishment of a Safe and Secure Ubiquitous Network Society

1. Consumer administration in relation to telecommunications services

(1) Promotion of ICT services that reflect the public viewpoint

Due to new ICT services and the distribution of information through new technologies which has created a need to clarify relations between such services and intellectual property and other rights, the MIC has held the Study Group Concerning Various Problems with ICT Services Based on User's Viewpoints since April 2009, and the group compiled and released its first draft proposal in August 2009 and second draft proposal in May 2010. In April 2009, four issues were decided upon, namely (1) Internet map information services, (2) illegal music distribution, (3), services utilizing LifeLog, and (4) revision of guidelines for protection of personal information, and the results of deliberations on (1)(2) and (4) were released as a draft proposal. In May 2010, the results of deliberations on issue (3) and on two new issues identified after the release of the first draft proposal ((5) CGM [Customer Generated Media], such as SNS and blogs, and (6) safety and security measures to be implemented when information is transferred onto mobile computers) were released as a second draft proposal.

(2) Promotion of consumer protections in the telecommunications services sector

The MIC formulated the Guidelines Telecommunications Business Act Consumer Protection Rules in March 2004 with the goal of making consumers secure when using telecommunication services, and in April 2010 put them into effect in conjunction with the enactment of the Telecommunications Business Act. In the report of the Panel on the Telecommunications Service Users prepared in February 2009, it was proposed that inclusion of contact information and means of contact, in case of change or dissolution of contracts, in explanations when contracts for telecommunications services are concluded, and recommendation of a basic policy of tailoring solicitations to the individual characteristics of users, be added to these guidelines. In response to this proposal, the Ordinance for Enforcement of the Telecommunications Business Act was partially revised in July 2009, and the Guidelines revised as well.

(3) 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 harmful information.

The MIC has been taking actions to deal with these issues, including the establishment of a consultation center to contact regarding harmful information, and will continue to take further steps in the future.

(4) Measures against nuisance e-mails

A wide variety of measures have been taken against nuisance e-mails, including the passage of the Act on Regulation of Transmission of Specified Electronic Mail and various voluntary efforts by the telecommunications sector. However, nuisance e-mail transmission methods have become increasingly devious and cunning, and the MIC is taking a wide variety of steps in response to the appearance of new problems such as the increasing number of nuisance e-mails sent from overseas. At the 171st session (2009 ordinary Diet session), the Establishment of Consumer Agency and Consumer Committee Act (Act No. 48 of 2009) was passed and went into effect on September 1.

With the establishment of the Consumer Affairs Agency and The Consumer Commission, the relevant regulations have been modified as well to give the Consumer Affairs Agency co-jurisdiction regarding the Law on Specified Electronic Mails as well. In line with this, the Law Enforcement Regulations Concerning the Guidelines for Sending of Special E-mail, etc. (2002 Ministry of Internal Affairs and Communications Act No. 66) has been revised as well.

(5) Protection of personal information in the telecommunications field

In order to improve the benefit of telecommunications services and protect the rights and interests of users, the MIC formulated the Guidelines for Protecting Personal Information in the Telecommunications Sector and Their Interpretation in August 2004, and enforces them. In August 2009, based on the initial recommendations of the Study Group Concerning the Various Problems with the ICT Service Based on User's Viewpoints, the Guidelines and Interpretation were revised in December 2009.

In August 2004, the MIC also formulated the Guidelines concerning the Protection of Personal Information of Broadcast Receivers (2004, Ministry of Internal Affairs and Communications Bulletin No. 696), enacted April 2005. These Guidelines were revised in July 2007 with consideration for developments since enactment, and revised again in September 2009 based on the partial revision of the Basic Policy on the Protection of Personal Information (April 2004, Cabinet Decision).

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 Center (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 2009, the NISC developed the Second National Strategy on Information Security covering the three years from 2009 to 2011 in a Security Policy Meeting. Also, based on this plan, the Secure Japan 2009 promotion program was finalized in June 2009.

In May 2010, the same Security Policy Meeting decided on the Information Security Strategy for the Protection of Citizens, aimed at responding effectively to environmental changes due to the increasing diversification, sophistication and complexity of information security. This is a comprehensive strategy for the four years from 2010 through 2013, incorporating the Second-Term Information Security Basic Plan. The NISC plans to release the Secure Japan 2010 annual plan which will be based on this strategy.

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

Based on 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 responsive to the increasing diversification of network-connected objects, and where people can use information and communications networks safely.

(3) Ensuring safety and reliability in the telecommunications services

In order to ensure the safety and reliability in the telecommunications services, the MIC has taken steps such as legal ordainment of the technical standards for equipment, imposition of requirements for selection of chief telecommunications engineers and reporting of maintenance provisions, and promotion of utilization of the guidelines "Standards for Security and Reliability of Information and Communication Networks" (1989, Ministry of Posts and Telecommunications Proclamation No. 73). In addition, in response to the recommendations of the Security Policy Meeting (office: Chief Cabinet Office, Information Security Center), the MIC supported the formulation of the Safety Criteria for Ensuring Information Security in the Telecommunications Sector and promotes their adoption by telecommunications operators.

While the conversion of networks to IP format progresses, transmission interference incidents are increasing in number, scale and duration. In response, the MIC held the IP Network Management Human Resources Study Group in April 2008, and compiled and released a final report in February 2009.

At disaster sites, the current public announcement system used by police, fire department, emergency rescue, etc., is an audio broadcast system, but in order to share accurate information such as on the status of affected areas, there is a need for a more flexible and dependable means of transmitting visual images.

To meet this need, in April 2009 the MIC advised the Information and Communications Council, on the basis of the Council's June 2007 findings, regarding the technological prerequisites for a mobile public disaster broadcast system, recommending the introduction of an independently operated broadband transmission-capable transmission system in order to realize a safe and secure society. Deliberations in the Council began in May 2009, and findings were released in March 2010. Based on these findings, in April 2010, proposals for revisions of relevant laws aimed at developing an environment conducive to a public broadband disaster broadcast system was presented to the Radio Regulatory Council.

(4) Safety assessment and promotion of advancement of cryptographic technology

In order to ensure information security, which is indispensable for network-based social and economic activities, it is essential to utilize safe and well-designed cryptographic technology.

To this end, CRYPTREC (Cryptography Research and Evaluation Committees), composed of the CRYPTREC Advisory Committee which is jointly constituted by the MIC and the Ministry of Economy, Trade and Industry (METI); the Cryptographic Technique Monitoring Subcommittee, and the Cryptographic Module Subcommittee, which are jointly constituted by the National Institute of Information and Communication Technology (NICT) and the Information-technology Promotion Agency, Japan (IPA), publicly invited ciphers, evaluated them objectively, and decided and publicized, in February, 2003, a list of recommended ciphers that should be recommended for their level of safety and superior design.

The CRYPTREC Advisory Committee evaluates cryptographic technology for use in e-government, etc., and in March 2009 compiled a list of publicly invited ciphers for updating of the e-Government Recommended Ciphers List, an FY 2002 list of ciphers that should be recommended for use in e-government procurement.