Section 5

Challenges Toward Achieving u-Japan

1 Safe and secure ICT use

(1) ICT security incidents experienced by individuals and companies

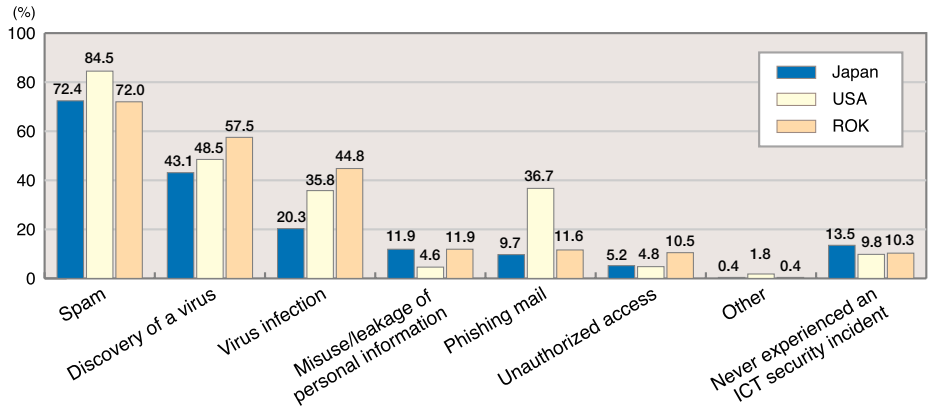
Among PC Internet users, 86.5% experienced ICT security incidents during 2004. The most frequently occurring incident was "spam" at 72.4%, followed by "discovery of a virus" (43.1%) and "virus infection" (20.3%).

A similar trend was observed in the United States and the Republic of Korea as well. About 90% of PC Internet users experienced some ICT security incidents, and the most frequently occurring incidents were in the order of "spam," "discovery of a virus," and "virus infection." Looking at the individual types of incidents, "virus infection" was most frequently observed in the Republic of Korea at 44.8%, followed by the United States at 35.8% and Japan at 20.3%. In the United States, where phishing has grown into a social problem recently, "phishing mail" was experienced by 36.7% of users, which is higher than the 9.7% in Japan and the 11.6% in the Republic of Korea **(Figure 1-5-1)**.

(2) Virus and unauthorized access

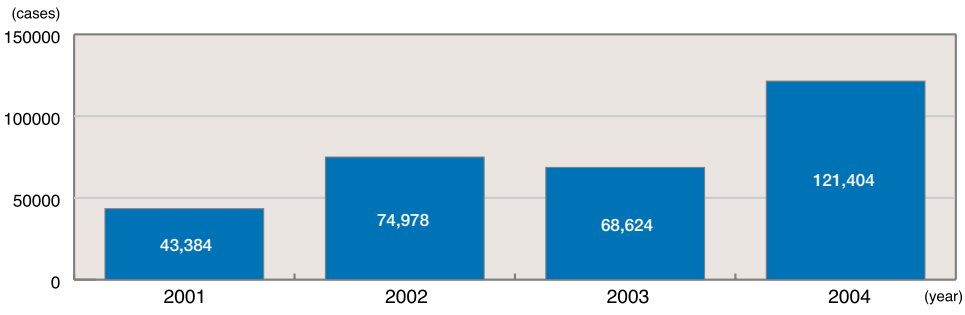
According to two companies aggregating and publishing virus incident reports, the number of virus incidents reported during 2004 was 121,404, which is about three times higher than the 43,384 incidents observed during 2001 **(Figure 1-5-2)**. In 2004, new viruses including "Netsky" and "Bagle" spread widely.

Figure 1-5-1 ICT security incidents experienced by PC Internet users



Source: Survey on Networks and People's Lives (Web Survey)

Figure 1-5-2 Transition in the number of virus incidents reported

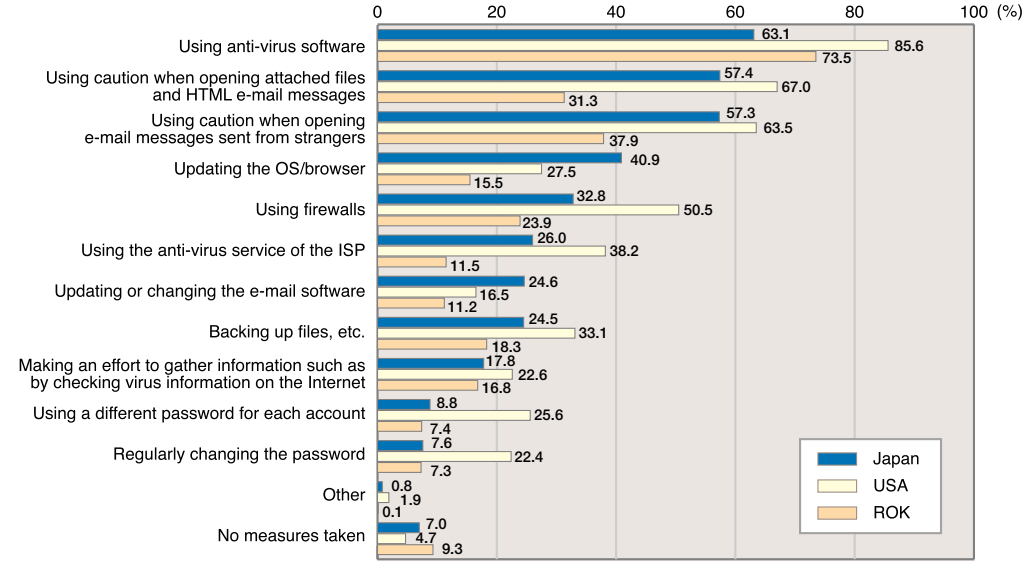


Source: Survey on Networks and People's Lives

Among Internet users, 93.0% take some measure against viruses and unauthorized accesses. The measure most frequently taken is “using anti-virus software” at 63.1%, followed by “using caution when opening attached files and HTML e-mail messages” (57.4%).

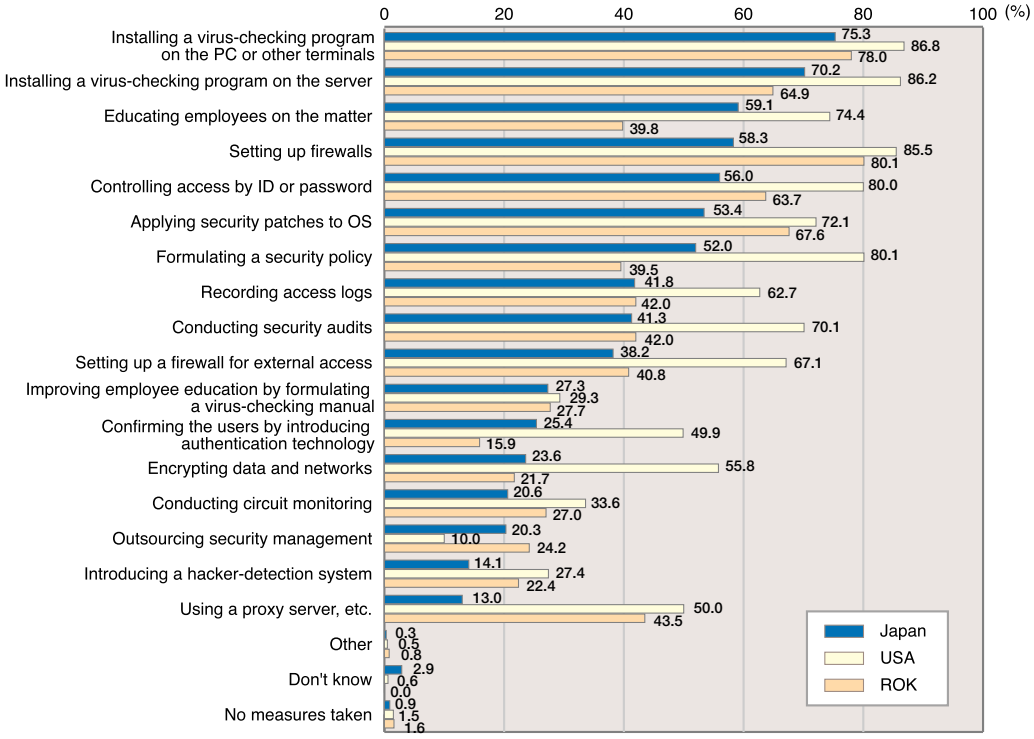
A similar trend is observed in the United States and the Republic of Korea as well. More than 90% of Internet users take some measure, and the most frequently taken measures include “using anti-virus software” and “using caution when opening attached files and HTML e-mail messages.” Overall, Internet users in the United States are taking the strongest measures, followed by users in Japan and users in the Republic of Korea **(Figure 1-5-3)**.

Figure 1-5-3 Anti-virus measures and measures against unauthorized access taken by Internet users



Source: Survey on Networks and People’s Lives (Web Survey)

Figure 1-5-4 IT security measures taken by companies



Source: Survey on the Current Status of ICT Use by Companies (Web Survey)

Companies taking some measure against ICT security incidents account for 99.1%. The most frequently taken measure is "installing a virus-checking program on the PC or other terminals" at 75.3%, followed by "installing a virus-checking program on the server" (70.2%), "educating employees on the matter" (59.1%), and "setting up firewalls" (58.3%).

Most companies in the United States and the Republic of Korea also take some measures. When comparing the status of implementation of concrete measures, the implementation rate is high for U.S. companies in most of the measures. In particular, U.S. companies are advanced in operational and institutional measures such as "educating employees on the matter," "formulating a security policy," and "conducting security audits" **(Figure 1-5-4)**.

(3) Spam

Indeed, 86.6% of PC users and 72.6% of mobile phone users have received spam in the past. While more than 70% of PC and mobile phone spam recipients receive five or less spam messages per day, more than 10% of PC spam recipients receive 11 messages or more per day.

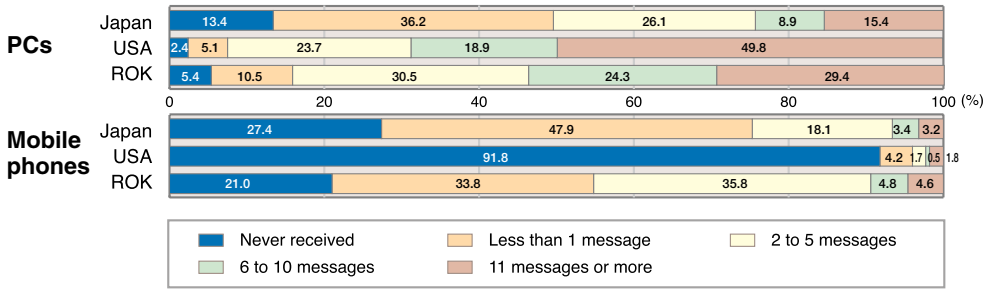
In the United States, only 8.2% of mobile phone users have received spam because mobile phone e-mail is not in wide use, but 97.6% of PC Internet users have received spam, and nearly half of them receive 11 spam messages or more per day. In the Republic of Korea, 94.6% of PC Internet users and 79.0% of mobile phone users have received spam, and the situation is generally the same as in Japan **(Figure 1-5-5)**.

(4) Protection of personal information

Among Internet users, 51.5% take some measures for protecting personal information. Specifically, the most frequently taken measure is "avoid disclosing personal information on the Internet" at 33.9%, followed by "avoid careless downloading of programs" (25.1%) and "refrain from entering credit card numbers" (23.7%) **(Figure 1-5-6)**.

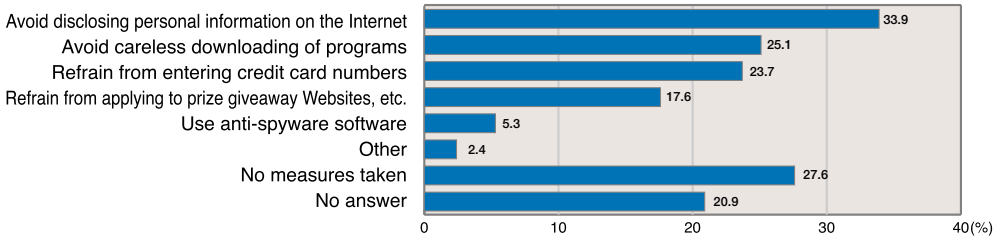
The Law Concerning the Protection of Personal Information came into force in April 2005, and business operators handling personal information became obligated to use personal information only for the specified purposes of use, acquire such information through appropriate means, and take measures for safely managing such

Figure 1-5-5 Number of spam messages received per day



Source: Survey on Networks and People's Lives (Web Survey)

Figure 1-5-6 Internet users' measures for protecting personal information (multiple responses possible)



Source: MIC, 2004 Communications Usage Trend Survey

information.

In these circumstances, companies' efforts for protecting personal information have made progress. When comparing companies' methods of managing personal information in FY 2003 and FY 2004, greater efforts are observed for all items. In particular, a considerably larger number of companies have come to "formulate personal information management rules and notify them to persons concerned" (49.7%) and "limit use and viewing of customers' personal information" (40.5%) **(Figure 1-5-7)**.

On the whole, measures against information leakage by insiders have also made progress. The most frequently taken measures are to "limit entrance into the server room" (74.7%) and "limit the removal of laptop PCs and OA equipment from premises" (49.7%) **(Figure 1-5-8)**.

(5) Challenges toward a ubiquitous network society

The "Policy Roundtable for Realizing a Ubiquitous Network Society" divided the challenges in the shadow of a ubiquitous network society into ten major divisions such as privacy protection and security, and listed ten individual challenges for each division, presenting a total of 100 challenges. Then, in order to clarify the priority challenges among these 100, it conducted a questionnaire survey on experts and extracted priority challenges based on two perspectives: the degree of impact on society and the degree of insufficiency of measures. As a result, 21 priority challenges were extracted including "vulnerability of ICT networks," "regional gaps in advanced services," and "illegal business practices using networks" **(Figure 1-5-9)**.

While a ubiquitous network society has positive effects such as enhancing safety, security, and convenience in people's lives, it also has negative effects such as the possibility of generating new problems related to privacy or security. Therefore, Internet users in Japan, the United States, and the Republic of Korea were asked whether or not construction of a ubiquitous network society, which has both positive effects and negative effects, should be promoted. In the three countries, the most chosen answers were those in support of promoting construction of a ubiquitous network society, but differences were observed in awareness in each country. In Japan, the percentage of respondents who answered

Figure 1-5-7 Companies' methods of managing personal information (multiple responses possible)

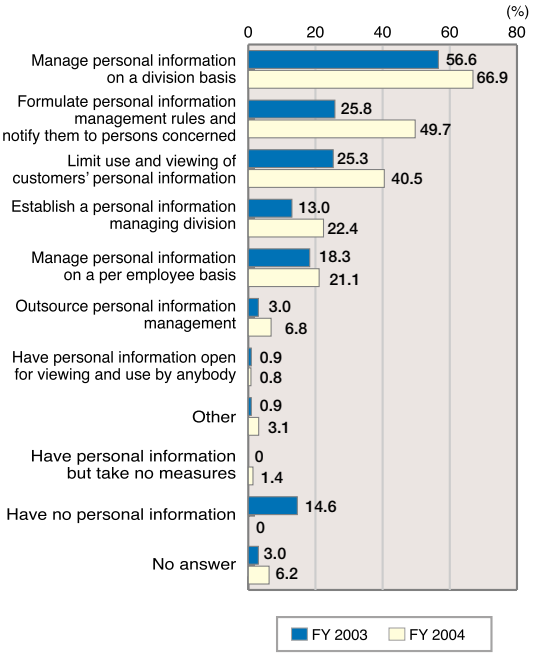
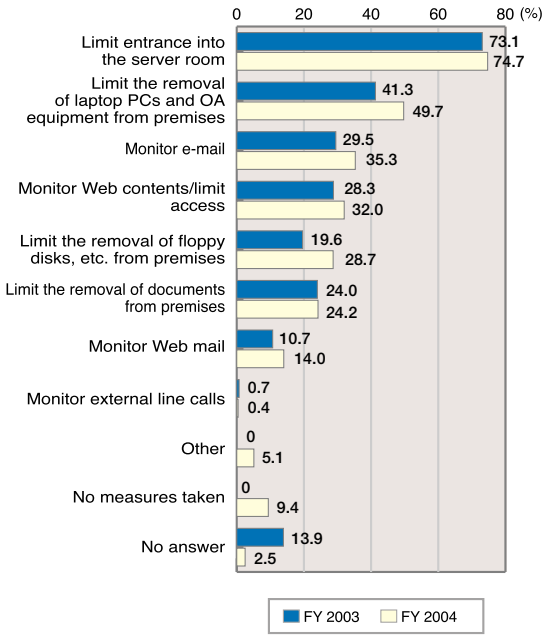
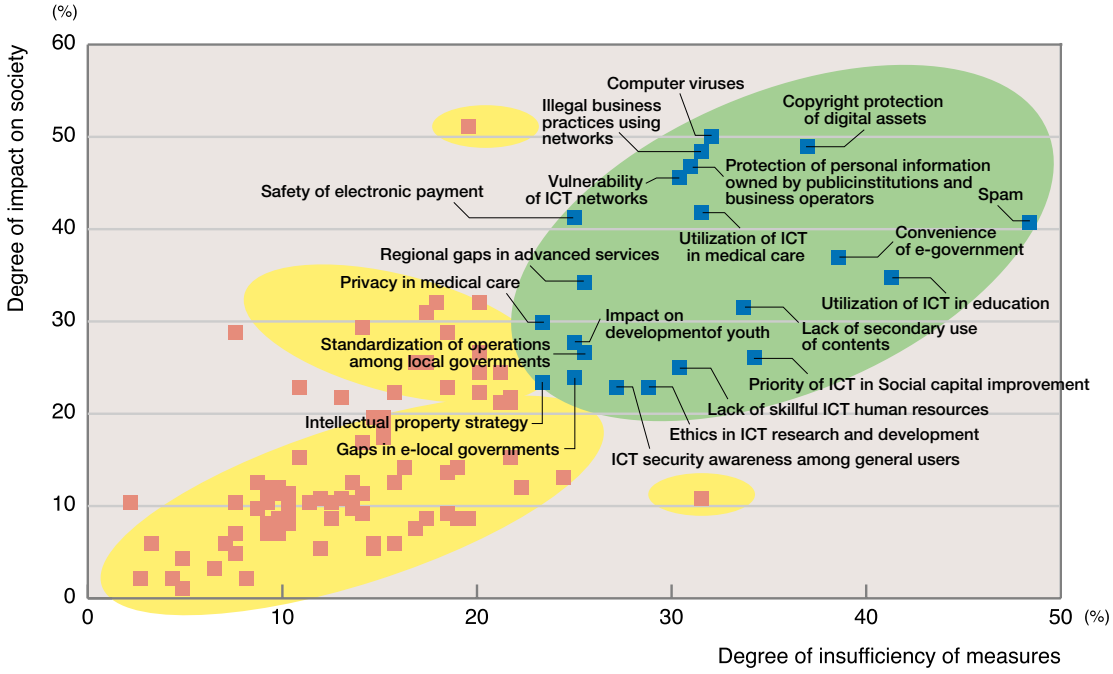


Figure 1-5-8 Measures against information leakage by insiders (multiple responses possible)



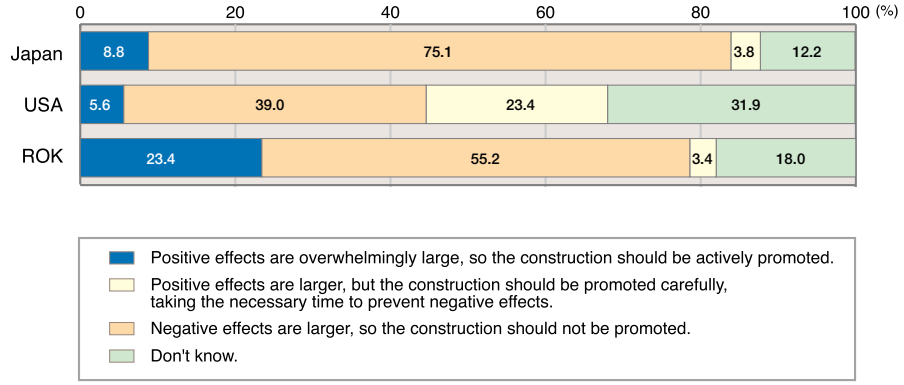
Source for Figures 1-5-7 and 1-5-8: Survey on the Status Trend of Information Security

Figure 1-5-9 Priority challenges toward a ubiquitous network society



Source: MIC, Final Report of the Policy Roundtable for Realizing a Ubiquitous Network Society

Figure 1-5-10 Approval/disapproval for construction of a ubiquitous network society

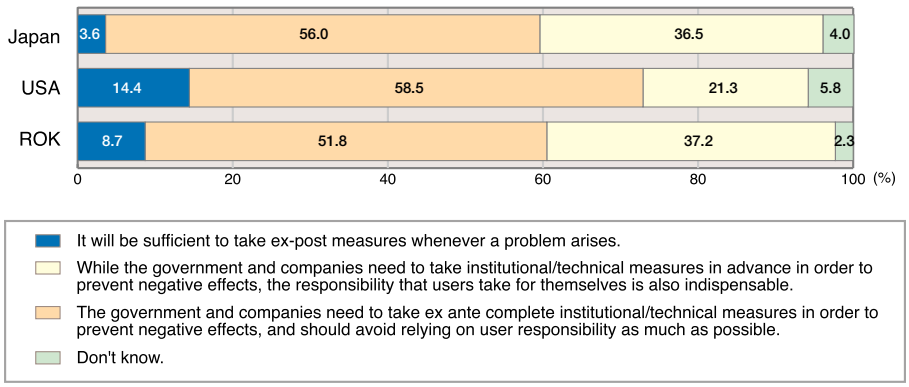


Source: Survey on Networks and People's Lives (Web Survey)

"positive effects are larger, but the construction should be promoted carefully, taking the necessary time to prevent negative effects" was 75.1%, which is higher than in the United States and the Republic of Korea. In the United States, the percentage of respondents who answered "negative effects are larger, so the construction should not be promoted" was 23.4%, which is considerably higher than in Japan and the Republic of Korea. In the Republic of Korea, the percentage of respondents who answered "positive effects are overwhelmingly large, so the construction should be actively promoted" was 23.4%, which is higher than in Japan and the United States **(Figure 1-5-10)**. This indicates that careful promotion is supported in Japan, a considerable number of people oppose the construction in the United States, and proactive promotion is supported in the Republic of Korea.

Furthermore, those who answered that construction of a ubiquitous network society should be promoted were asked about measures against the negative effects. In Japan, the United States, and the Republic of Korea, the most chosen answer was "while the government and companies need to take institutional/technical measures in advance in order to prevent negative effects, the responsibility that users take for themselves is also indispensable." Meanwhile, in Japan and the Republic of Korea, more respondents answered "the government and companies need to take ex ante complete institutional/technical measures in order to prevent negative effects, and should avoid relying on user responsibility as much as possible" than in the United States. In the United States, more respondents answered "it will be sufficient to take ex-post measures whenever a problem arises" than in Japan and the Republic of Korea. The awareness of user responsibility tends to be stronger in the United States than in the other two countries **(Figure 1-5-11)**.

Figure 1-5-11 Opinions on measures against the negative effects of a ubiquitous network society



Source: Survey on Networks and People's Lives (Web Survey)

2 Current status of the digital divide

Looking at the diffusion of major broadband services by population of the municipality, ADSL is diffused to 100% of municipalities with a population of over 50,000, 92.3% of those with a population of over 5,000 and up to 10,000, and 54.7% of those with a population of 5,000 or less. Meanwhile, FTTH is diffused to 93.1% of municipalities with a population of over 50,000, but only to 11.6% of those with a population of over 5,000 and up to 10,000, and 3.0% of those with a population of 5,000 or less. In this manner, there are gaps in diffusion between municipalities according to their population, and the gaps are considerably wide for FTTH **(Figure 1-5-12)**.

3 Backbone circuit

(1) Surge in Internet traffic

The MIC conducted an aggregation and trial calculation of Japan's Internet traffic data with the cooperation of seven ISPs (September - November 2004) and the academic world.

The traffic of broadband subscribers has been constantly increasing. Since the difference between the downloading traffic (traffic from ISPs to subscribers) and the uploading traffic (traffic from subscribers to ISPs) is becoming smaller, ISPs can no longer construct their networks with a premise that "general users mainly use downloading services" **(Figure 1-5-13)**.

Since traffic exchanges between the seven ISPs and other ISPs are more frequently conducted through private peering, etc. than through major domestic Internet Exchanges (IXs), the traffic data for major domestic IXs are insufficient for estimating the total amount of traffic exchanged **(Figure 1-5-14)**.

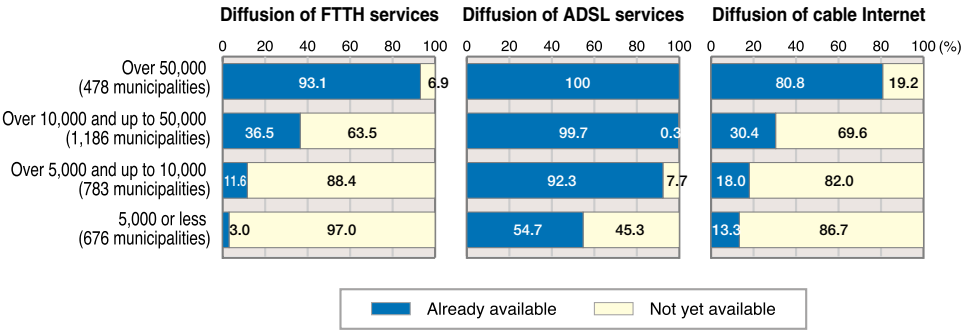
When the total amount of traffic of broadband subscribers in Japan was estimated based on the seven ISPs' 41.1% share of the total "In" traffic at the major domestic IXs (the total amount of traffic coming in from subscribers to the major domestic IXs) and the 133.0 Gbps traffic from the broadband subscribers of the seven ISPs, it was assessed that traffic exceeding 300 Gpbs (133.0 Gpbs / 41.1% = 323.6 Gpbs) is moving on the Internet.

(2) Concentration of Internet traffic exchanges in Tokyo

According to a questionnaire survey conducted by the MIC on the 14 major ISPs (February 2004), IXs' total circuit capacity for public peering was 230.4 Gpbs, out of which about 80% were concentrated in Tokyo. Meanwhile, the total circuit capacity for private peering was 278.2 Gpbs, out of which about 90% were concentrated in Tokyo.

Due to the concentration of traffic exchanges in Tokyo, various problems are being pointed out, such as deterioration of broadband services in the region and the vulnerability to cyber attacks and large-scale disasters. While many major ISPs and IXs conduct traffic exchanges not only in Tokyo, but also in Osaka, etc. for risk management, it would also be necessary to examine the technical problems in shifting to a distributed network mode in order to achieve stable operation of the whole Internet.

Figure 1-5-12 Diffusion of broadband services by population of the municipality (as of the end of March 2005)



* The broadband services refer to ADSL, FTTH, cable Internet, and FWA.

Figure 1-5-13 Traffic by type of subscribers (transition in the average monthly traffic from September to November 2004; Gbps)

	In*	Out*
Broadband (DSL, FTTH) subscribers of seven ISPs	98.1 → 108.3 → 116.0	118.1 → 124.9 → 133.0
Other (dial-up, dedicated line, data center) subscribers of four ISPs	14.0 → 15.0 → 16.2	13.6 → 14.9 → 15.6

* "In" indicates the traffic coming in from subscribers to the seven (or four) ISPs (uploading), while "Out" indicates the traffic going out from the seven (or four) ISPs to subscribers (downloading).

Figure 1-5-14 Traffic exchanges between ISPs (transition in the average monthly traffic from September to November 2004; Gbps)

	In*	Out*
Seven ISPs' traffic exchanges through major domestic IXs	35.9 → 36.3 → 38.0	30.9 → 31.8 → 33.0
Seven ISPs' other modes of traffic exchanges with domestic ISPs	48.2 → 53.1 → 55.1	37.8 → 41.6 → 43.3
Seven ISPs' traffic exchanges with overseas ISPs	25.3 → 27.7 → 28.5	14.1 → 15.4 → 16.7

* "In" indicates the traffic coming in to the seven ISPs, while "Out" indicates the traffic going out from the seven ISPs.