Section 5

Ensuring Information Security and Building a Securer IT Society

1. Necessity of Ensuring Information Security

The diffusion of information and communications, such as the Internet and e-commerce, and advancement of information and communications, such as broadband and mobile work, not only enhance convenience, but also increase information security risks. Accordingly, security measures are now the top priority issue in using information and communications networks. Among individuals' concerns/dissatisfactions in using the Internet, the most cited concern was "privacy protection" (54.1%), followed by "virus infection" (41.4%) (**Figure 1-47**). Of the problems companies face in using information and communications networks, the most mentioned problem was the "difficulty of setting up security measures" (69.7%), followed by "concerns about virus infection" (63.6%) (**Figure 1-48**).

With further progress of information and communications, the damages inflicted by information security infringements may become even greater. As the OECD recommends, there is a strong need to promptly establish "a Culture of Security" under which all people involved in information and communications recognize the need and measures for ensuring information security, assuming every possible risk.

2. Trends in Information Security Infringements, etc.

Combining the reported number of virus incidents released by two companies aggregating such reports, the number has almost doubled from 37,622 cases in 2001 to

Figure 1-47: Individuals' Concerns/Dissatisfactions Related to Internet Use (multiple answers)

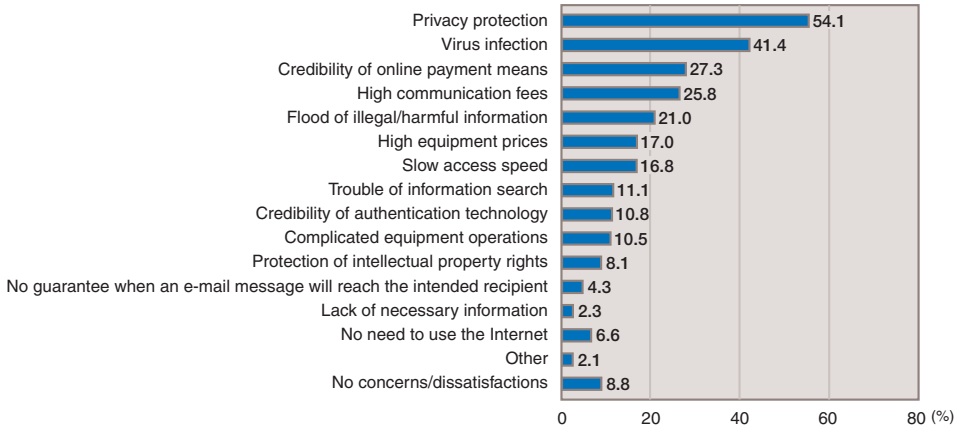
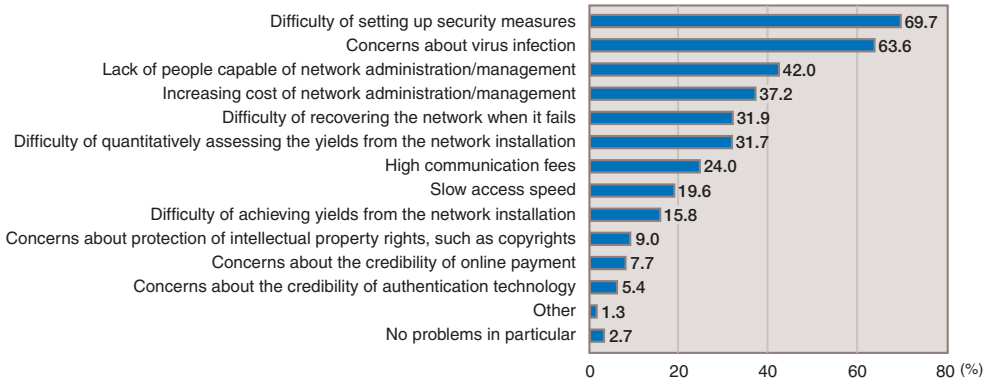


Figure 1-48: Problems Companies Face in Using Information and Communications Networks (multiple answers)



Source (Figures 1-47&1-48): "Communications Usage Trend Survey in 2002," MPHPT.

74,001 cases in 2002.

Also, according to the announcement by the National Public Safety Commission, the Ministry of Public Management, Home Affairs, Posts and Telecommunications (MPHPT), and the Ministry of Economy, Trade and Industry (METI), the number of unauthorized accesses recognized in 2002 totaled 329, making a dramatic decrease of 924 cases from 1,253 cases in 2001. Although attacks on security holes using Web page rewriting programs were observed in large numbers in 2001, the number is considered to have decreased in 2002 due to the recent publicity activities by public and private sectors and diffusion of security patches.

"Spam," which is e-mail sent to a user without the user's consent for the purpose of advertising, sales promotion, and solicitation, suddenly increased around June 2001, and the number of complaints and inquiries to cell phone carriers increased accordingly. In a survey conducted at the end of 2002, 58.0% of mobile Internet users and 15.5% of Internet users accessing from PCs received spam in the past one year; the occurrence of spam incidents is particularly high for the mobile Internet.

3. Status of Internet Security Incidents

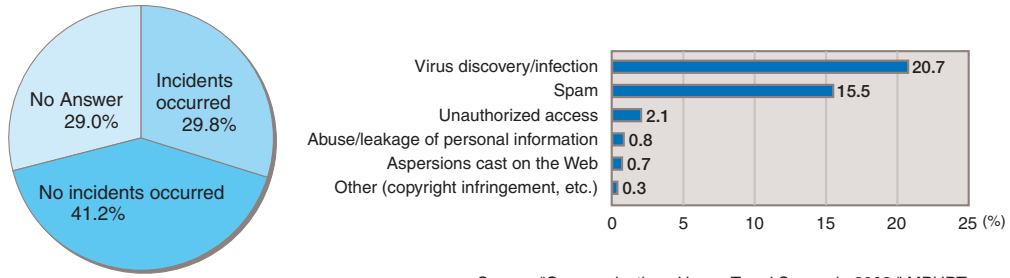
(1) Status of security incidents suffered by individuals

The proportion of those who suffered information security incidents during 2002 was 29.8%, almost 30%, of all Internet users accessing from PCs. The most reported incident was "virus discovery/infection," suffered by 20.7% of the Internet users accessing from PCs. This was followed by "spam" suffered by 15.5% and "unauthorized access" suffered by 2.1%. "Abuse/leakage of personal information" was experienced by 0.8% (**Figure 1-49**). Those who not only discovered, but were actually infected by viruses accounted for 10.4%.

(2) Status of security incidents suffered by companies

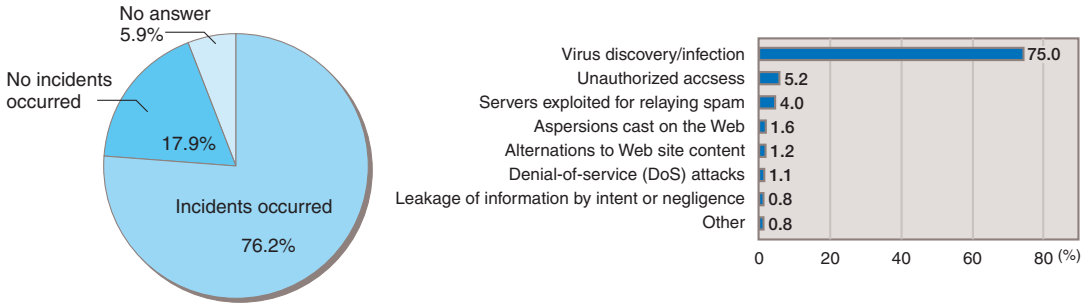
During 2002, 76.2%, approximately three-quarters, of companies suffered some kind of information security incident in using information and communications networks (the Internet and corporate communication networks). The top-ranking incident was "virus

Figure 1-49: Situation and Types of Security Incidents Suffered by Internet Users Accessing from PCs (multiple answers; for the past one year)



Source: "Communications Usage Trend Survey in 2002," MPHPT.

Figure 1-50: Situation and Types of Security Incidents on Information and Communications Networks Suffered by Companies in 2002 (multiple answers)



Source: "Communications Usage Trend Survey in 2002," MPHPT.

discovery/infection" suffered by 75.0% of all companies. This was followed by "unauthorized access" experienced by 5.2% and "servers exploited for relaying spam" suffered by 4.0% (**Figure 1-50**).

Companies that did not only discover, but were actually infected by viruses accounted for 43.5%.

(3) Estimated amount of damages suffered by individuals and companies

(i) Estimated amount of damages suffered by individuals

According to a sample survey on the rates and amounts of damages suffered, the amount of damages suffered by individuals from virus incidents and unauthorized accesses in 2002 is estimated to be approximately 41.7 billion yen in total. Of this amount, damages from "virus incidents" accounted for about 38.4 billion yen and damages from "unauthorized accesses" accounted for about 3.3 billion yen (**Figure 1-51**).

This amount only totals the estimated amount of damages from virus incidents and unauthorized accesses related to PCs, and does not include such damages suffered from aspersions cast on the Web and spam sent to cell phones. This amount is solely the actual amount paid for repairing or replacing broken PCs, etc.

(ii) Estimated amount of damages suffered by companies

According to a sample survey on the rates and amounts of damages suffered, the amount of damages suffered by companies from information security incidents in 2002 is estimated to be approximately 346.5 billion yen. The largest damages were inflicted by "virus infection" at about 302.7 billion yen, followed by "system crashes, server failures" at about 40.8 billion yen, "alteration to Web site content" at about 1.9 billion yen, "aspersions cast on the Web" at about 700 million yen, and "stealing/leakage of customer information" at about 500 million yen (**Figure 1-52**).

This amount only totals the estimated amount of investigation/restoration costs and lost earnings, and does not include such damages as collapse of credit resulting from harmful rumors.

4. Information Security Measures and Future Tasks

(1) Measures and future tasks of individuals

The top measure against viruses and unauthorized accesses taken by Internet users was "installation of

Figure 1-51: Estimated Amount of Damages from Information Security Incidents Suffered by Individuals in 2002

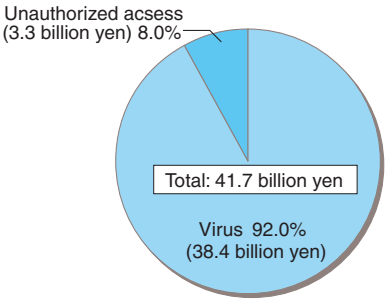
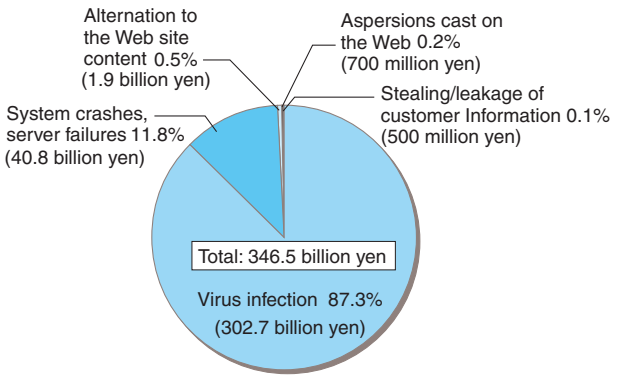
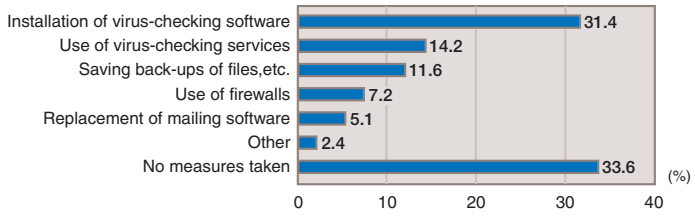


Figure 1-52: Estimated Amount of Damages from Information Security Incidents Suffered by Companies in 2002



Source (Figures 1-51&1-52): "Survey on Content and Security."

Figure 1-53: Status of Information Security Measures Taken by Internet Users (multiple answers)



Source : "Survey on Content and Security."

virus-checking software" at 31.4%, followed by "use of virus-checking services" at 14.2%, and "saving back-ups of files, etc." at 11.6%. However, those who answered "no measures taken" accounted for 33.6%, approximately one-third of the total (**Figure 1-53**).

In this manner, there are a certain number of people who have not taken any information security measures. When they were asked the reason for not taking such measures, 86.5% of them answered that they had not taken any measures despite being aware of the need. Since 65.3% of those who had not taken any information security measures gave "lack of know-how of concrete security measures" as the reason, the future task in promoting information security measures among individuals would be to increase people's knowledge of information security (**Figure 1-54**).

(2) Measures and future tasks of companies

(i) Status of information security measures

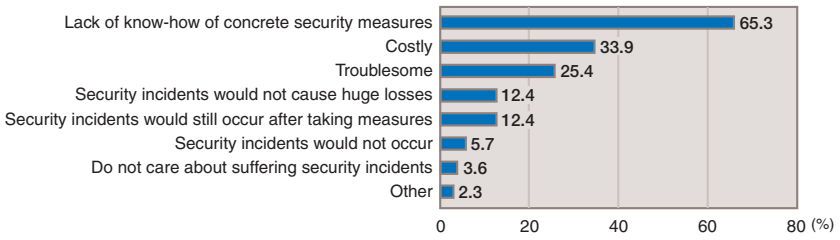
With regard to the status of information security measures taken by companies in 2002, the most taken measure was "installation of virus-checking software on PCs and other terminals" implemented by 83.8% of all companies. "Use of firewalls" was implemented by 52.0%, about half of all companies. Companies that were "taking no measure in particular" were only 2.2%, indicating that most companies implemented some kind of measures (**Figure 1-55**).

(ii) Information security management

In order for companies to fully bring out the effect of information security measures, companies need to repeat the "PDCA cycle" consisting of [1] planning of security policies, etc. (PLAN), [2] implementation of measures (DO), [3] verification of the effects and efficacy of the measures (CHECK), and [4] review of the measures (ACTION), as information security management.

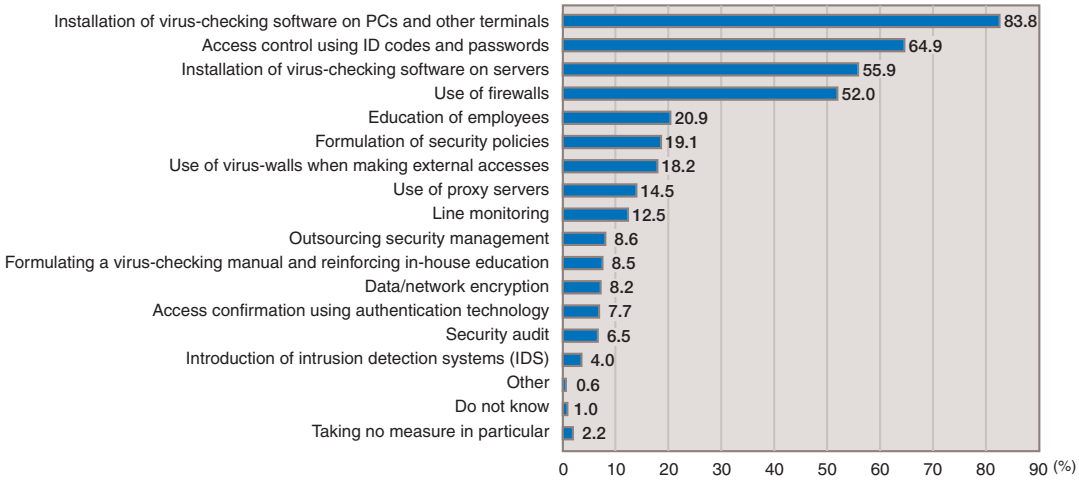
According to a survey on self-evaluation of the status of engagement in the respective phases of the cycle, the proportion of companies that answered "largely implemented" was relatively high for DO (41.4%) and PLAN (31.7%). However, the proportion was low for CHECK (19.3%) and ACTION (13.9%). The future task for enhancing information security measures in companies would be to make more efforts in verifying the effect of the measures and reviewing the measures.

Figure 1-54: Reasons for Not Taking Information Security Measures (multiple answers)



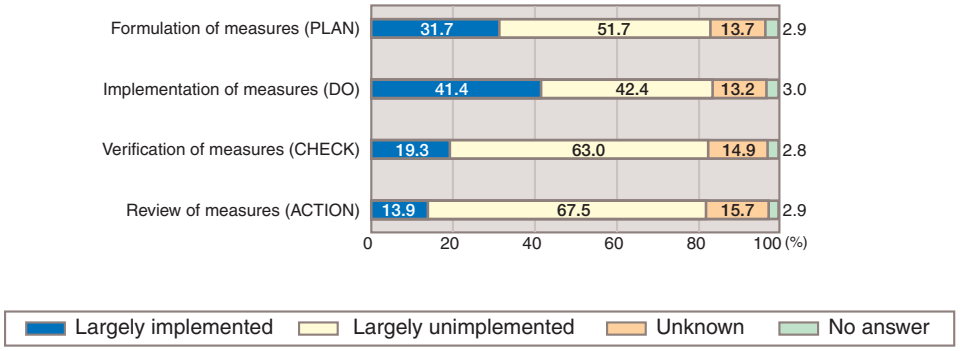
Source: "Survey on Content and Security."

Figure 1-55: Status of Information Security Measures Taken by Companies (multiple answers)



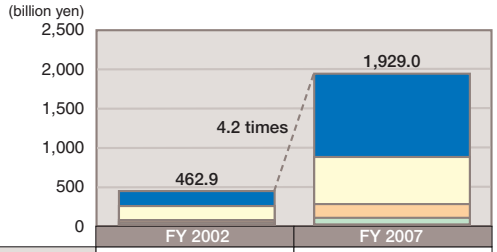
Source: "Communications Usage Trend Survey in 2002," MPHPT.

Figure 1-56: Evaluation of Companies' Engagement in the Information Security Management Cycle



Source: "Survey on Content and Security."

Figure 1-57: Current Status and Prediction of the Market Size of Information Security Business



	FY 2002	FY 2007
Supplying information security-related products	259.5	1,080.9
Information security services	161.8	676.4
Consulting	28.9	116.1
Information security evaluation	12.7	55.6
Total	462.9	1,929.0

Source: "Survey on Content and Security."

5. Trends in Information Security Business

The estimated market size of information security business in fiscal 2002 is 462.9 billion yen. In the market, supply of information security-related equipment and software accounted for 259.5 billion yen, which is 56.1% of the total. This was followed by information security services accounting for 161.8 billion yen, 35.0% of the total. According to the predictions by security business operators, the market size of information security business is estimated to become 1.93 trillion yen in fiscal 2007, growing by 4.2 times the size in fiscal 2002 (**Figure 1-57**).

6. Safety and Reliability of the Information and Communications Networks

Recent years have seen the occurrence of not only security infringements of individuals and companies, but also infringements that threaten overall information and communications networks. Because the society and economy in general have come to depend increasingly on information and communications networks these days, if the safety and reliability of information and communications networks were undermined, the resulting damage could be enormous.

The safety and reliability of information and communications networks have been threatened many times in

the past by natural disasters, such as great earthquakes. However, in addition to such natural disasters, the safety and reliability of information and communications networks have actually been infringed by human-caused attacks, such as cyber terrorism, in recent years.

(1) Internet failure caused by the SQL Slammer

In January 2003, a worm virus called the SQL Slammer raged, causing the largest-ever Internet failure. Although Japan did not suffer notable damages except in part, the United States, the Republic of Korea, and China suffered great damages. In the Republic of Korea, in particular, the Internet stopped for about nine hours nationwide and caused social confusion.

(2) Attacks on route name servers

In October 2002, route name servers in 13 locations worldwide simultaneously received DDoS attacks (distributed denial of service: attacks of simultaneously sending massive quantities of data by using many relay servers with the aim of failing the target system). Although no actual damage was caused to general users, the processing power of route name servers in nine locations in Japan, the United States, etc. showed a slight decline.

(3) Functional disorders of telecommunications networks cause by "wangiri" calls

Incidents of “wangiri” calls suddenly increased from around November 2001. A “wangiri” call is a nuisance call abusing the number display function of cell phone terminals, etc. It is an act of hanging up after only making a single call in order to have the user call back the number left in the call record and listen to paid voice services. In July 2002, NTT WEST suffered an incident in which a tremendous number of “wangiri” calls caused congestion in part of Osaka and Hyogo, and obstructed use of about five million telephone lines.

7. Measures Taken in Other Countries

In order to counter the risks against information security and information and communications networks, the Japanese government has been taking various measures by establishing the “IT Security Promotion Committee” and the “IT Security Expert Meeting in the IT Strategic Headquarters.” The MPHPT has also taken such actions as amending the Wire Telecommunications Law, holding the “Study Group for Ensuring Important Telecommunications in the Telecommunications Business,” and promoting related technological development. After the simutaneous terrorist attacks in the United States in September 11, 2001, the awareness of ensuring national security has risen and information security policies have been strengthened in international organizations, the United States, and the EU.