Toward the Establishment of a Safe, Secure Internet Society through International Cooperation

Proposals to the 1st Internet Governance forum(IGF)

Nippon Keidanren
(Japan Business Federation)

October 25, 2006

Toward the Establishment of a Safe, Secure Internet Society through International Cooperation
Proposals to the 1st Internet Governance Forum (IGF)

1. Introduction

1. The role of the IGF

A free and open Internet has flourished under private-sector management, and building a safer, more secure environment for Internet users is an issue of the highest priority for the international community. This and related issues are already under consideration within multilateral groupings including the G8, OECD, and EU. The IGF is a gathering of multi-stakeholders from various countries around the world, and is a unique opportunity to raise awareness, share ideas and experiences and build more understanding regarding Internet governance issues within the international community. Making the most of this position, the IGF should accumulate the knowledge of international organizations, governments, private sector, civil society, and technical experts to build more understanding regarding the measures that will be required, and should promote the sharing of best practices. Issues that require the international community to work together in partnership include achieving a safe, secure Internet society (security and spam prevention measures and so on), and providing the social and cultural infrastructure needed to support proper use of the Internet (security training, the issue of balance between freedom of expression and content discipline and so on). Also the IGF is expected to fulfill the function of creating a virtuous cycle in which the significant outcomes of activities undertaken by international organizations and other existing groups are shared, and where discussion at the IGF becomes a source of reference for each organization, enhancing its problem-solving capabilities.

2. Expectations of the 1st IGF

Nippon Keidanren believes that both matters in need of urgent consideration and fundamental issues concerning the development of the Internet society should be given priority at the 1st IGF. It is important to discuss establishing an Internet environment that can be trusted -- an issue that was not covered sufficiently by WSIS. The themes set for the current forum[1] closely match those proposed by Nippon Keidanren, and we appreciate the selection of issues.

Nippon Keidanren believes that a free and open Internet under private-sector management is the foundation of the development of today's information society, and that the current governance framework should be maintained in the future. However, the current situation in which viruses, phishing, spam and other problems interfere with safe and secure Internet use cannot be left

---

[1] Overall theme: Internet Governance for Development   Four separate themes: Openness, Security, Diversity, and Access

unaddressed, and the world of the Internet must be prevented from becoming a lawless zone. Consequently, Nippon Keidanren would like to make specific proposals to the 1st IGF for measures calculated to realize an Internet society in which anyone can use the Internet freely, without anxiety, while maintaining a proper balance between freedom and openness on the one hand, and safety and peace of mind on the other.

Because the establishment of a safe and secure Internet environment cannot result from separate approaches by each country, it is important to exchange at the IGF the viewpoints and information that emerge from the insights of the nations and all stakeholders participating. For example, since Internet crime is typically not limited by national boundaries, when just one country has a weakness in security measure, that country could logically become a haven for crime. Furthermore, when bots[2] and similar technologies are used to commit abuse, users may unwittingly become party to crimes and therefore, without the participation of all parties concerned including users, satisfactory results cannot be obtained.

In order to ensure that the Internet society develops in a sustainable manner, a safe and secure Internet environment must be established. To achieve this goal will require the active cooperation of international organizations, governments in each region of the world, private sector, technical experts and civil society. Joint action by all stakeholders in the international community is essential for solving these problems. Nippon Keidanren would like to propose the following recommendations to help to achieve this cooperation.

Japan, a nation that has taken the lead in offering broadband access, has been the first to experience a number of phenomena such as the measures taken against spam, improper and malignant use of P2P[3] file sharing software and so on. These occurrences have been recorded as case studies; as other countries move to implement wider broadband access, we hope that they will be put to good use, either as best practices to be followed or as examples to avoid.

---

[2] A program that is installed on a user's PC without his or her knowledge, which operates according to commands sent by its author. It is thought that nearly all unsolicited e-mail and DDoS attacks are controlled using bots.
[3] A method of using the Internet to exchange data directly between parties without involving a server, and applications that use this technology.

II. Proposals for the Establishment of a Safe, Secure Internet Society

1. Implementation of new international cooperation to ensure security

(1) Establish an international information sharing system

Where there are countries and regions in which the level of security is lagging, criminals will exploit the systems and equipment in those regions as the infrastructure for launching cyber attacks using bots and the like. In this situation, it is impossible for one country acting alone to take measures sufficient to ensure security. Therefore, the international community must work together to share information on incidents and the know-how developed in dealing with them, as well as in establishing a framework for cooperative security measures.[4]

We consider FIRST (Forum of Incident Response and Security Teams[5]) to be an effective framework for international information sharing, since its objective is exchanging security information between the CSIRT[6] of member countries, providing rapid notice of security incidents, and adopting measures against current and future threats. Those countries and regions that do not have CSIRT should proactively consider establishing a National CSIRT. International organizations, advanced countries and so on should provide support[7] in the form of human resources and know-how to unprepared countries and regions.

(2) Ensuring traceability

Cyber crime exploits the anonymous nature of the Internet, so in many cases it is difficult to trace abusers. For this reason, it is important to ensure the traceability of users.[8]

Typically, WHOIS[9] systems are used for confirming the identity of a user, but they do not necessarily contain accurate information, and when an incident occurs it is often difficult to make contact with the parties concerned. Accordingly, as part of the activities of the entities responsible for Internet governance, establishing[10] an effective system for contacting relevant parties, including an obligation to register accurate information in the WHOIS and update it regularly (annually, for example), would be extremely beneficial in achieving a quick response to incidents. However, this is only one means of ensuring traceability, and it is desirable to limit the items required for registration from the point of view of protecting privacy, and to impose stringent conditions on referencing information that has a bearing on privacy.

---

[4] In regions where the necessary legal framework is lacking, there is little risk in launching cyber attacks. This makes those regions prone to be targeted by criminals. It is therefore also important to establish international law on cyber crime.

[5] http://www.first.org/

[6] Acronym for "Computer Security Incident Response Team." The name of an organization that receives and investigates reports of computer security incidents, and implements countermeasures.

[7] Rather than providing financial assistance, it is more important to provide developing countries with the framework, know-how, and models of security measures that advanced countries possess. In addition, providing this sort of assistance raises the level of Internet security overall, resulting in benefits to all users connected to the Internet. Moreover, JPCERT/CC is taking proactive steps to support the establishment of CSIRT in a number of Asian countries.

[8] Although it may not be possible to ensure traceability of parties who intentionally commit criminal acts even if the measures in this proposal are implemented, they can be expected to provide a solution to unintended attacks from users through the agency of bots.

[9] A service that allows Internet users to reference information concerning the registrants of domain names and IP addresses. The service is provided by a registry or registrar.

[10] Today, registration is typically through a registration agent, but even in that case, traceability can be maintained if the agent registers accurate information.

Furthermore, in order to specify senders of e-mail with nefarious purposes, it would be effective to undertake registration to enable reverse DNS lookup[11] on an international basis.

(3) Coordinated measures against spam

Today, more than half of all the e-mail people receive is spam. Spam places a significant burden on networks and greatly inconveniences on Internet users. Furthermore, spam is also employed to induce users to visit phishing sites, the eradication of which is a pressing issue.

In order to respond to spam, as with other general security measures, it is necessary to implement multifaceted countermeasures in the areas of legislation, technology, education and consciousness-raising, based on cooperation between the relevant parties and with the roles shared appropriately. For example, the role of government is to implement effective regulations against unsolicited e-mail by prohibiting transmission of e-mail under a false address and so on. The role of private enterprise is to implement the latest technical measures like sender domain authentication[12] and Port 25 blocking[13], as well as to share information about malicious operators to prevent the spread of damage. We consider that signaling a clear intent to eradicate spam based on close cooperation between these two sectors must form the cornerstone of measures against nuisance e-mail, in conjunction with raising awareness of users to enhance their abilities to combat spam. Moreover, if measures of this sort are not taken on a worldwide scale, we cannot expect to see the eradication of spam from the Internet environment that we all use. Looking to the future, it will be necessary to exchange information about the responses required through a variety of channels, and implement suitable countermeasures.

Section III looks at the success of measures to eradicate spam in Japan's mobile phone networks.

2. Provide the social and cultural infrastructure needed to support proper use of the Internet

(1) Bridging the digital divide through capacity building

In order to narrow the digital divide between developed countries and developing countries, it is necessary to carry out education programs in developing countries to improve general familiarity with ICT in addition to providing infrastructure. In doing so, we must build and reinforce partnerships between governments, private sector, and civil society, focusing on existing international organizations, to provide an environment where anyone in the world can use ICT.

---

[11] Finding the domain name that corresponds to an IP address. In many cases, the data enabling this reverse lookup is not set.

[12] A technique for authenticating the server information (domain) of the source of e-mail at the receiving server. This enables a countermeasure whereby only e-mail from an identifiable sender is received. However there are currently still issues such as the lack of reliability in correctly authenticating all senders, so this approach requires further study.

[13] A countermeasure in which an ISP restricts access to Port 25, thereby blocking e-mail that does not pass through its own mail server. This approach is thought to be an effective measure against spam being transmitted by "zombie PCs" infected with a spambot.

(2) Promoting a culture of security

It would not be true to say that a culture of security[14] is sufficiently widespread even in developed countries. In Japan, too, compared with education in basic computer literacy, the level of education in security against the risks of Internet use is still insufficient. Looking to the future and the age of teleworking and remote medical care, the importance of this culture will only increase. For example, it is widely known that in order to prevent infection by computer viruses, it is important to use anti-virus software and the appropriate virus definition updates, as well as to avoid running files of unknown origin. However, the fact that there still seems to be no end to infected users points to a low level of recognition of information security on the part of users, considering the seriousness of security issues. Recently there has been a marked increase in infection by bots where the victims themselves, without knowing it, become perpetrators of crime. Therefore, if the number of users increases while the level of education and awareness of security remains insufficient, the dangers of using the Internet will simply become more widespread. Since this is also a required field in lifelong education, we must accumulate experience in effective methods of providing information, using animated web pages and other means to promote awareness.

On the other hand, if education programs as part of assistance to developing countries consist only of teaching people how to use ICT, it will only result in a worsening of security issues on a worldwide scale. Accordingly, the security aspects of ICT must be made one of the core elements of education and training so that assistance includes establishing the rules of behavior as well as the skills involved. It is important that this stance is incorporated into assistance from national governments and private organizations. In addition, the National CSIRT mentioned above may be a suitable entity for carrying out education and awareness training in security, and advanced countries should provide human resources and know-how for this purpose and should promote joint development of relevant teaching materials.

(3) Enhancing professional development for high-level information security

In addition to raising the level of competence of security personnel, it is also necessary to undertake the professional development of high-level information security personnel in order to enhance the capacity to respond to increasingly sophisticated attacks. Many countries have made the development of sophisticated ICT personnel a key piece of their national strategies. However, to this policy we must add professional development of high-level information security personnel who can assist in developing the Internet society of the future, as well as establishing a framework for international cooperation that will facilitate personnel development of this kind.

(4) Balance between freedom and regulation

Open access to the Internet and freedom of expression are essential to the development of the Internet Society, and these factors should be accorded the highest respect, as far as they are not in opposition to restrictions required for maintaining public morality.

---

[14] The OECD (Organisation for Economic Co-operation and Development) continues to take action to promote a "Culture of Security."

Accordingly, if for example filtering is applied to harmful sites, the criteria for putting sites on a blacklist must be explained clearly, and in setting these criteria, it is important for businesses providing filtering services and other related organizations to hold consultations on a regular basis.

At the same time, in some cases, it is inevitable that freedom will be restricted with the implementation of security measures. There is, at present, no clear answer to the question of how best to balance freedom and regulation for safety, and we must endeavor to reach broader understanding through discussion at the IGF.

III. Examples from Japan

In Japan, the development of ubiquitous networks through advances in mobile and broadband environments and the spread of electronic tags and the like have been accompanied by incidents of a kind never seen before. We would like to present these to the IGF as a helpful reference for the various countries of the world in which broadband access is becoming commonplace, and users are increasingly connecting to the Internet using mobile devices.

1. Reducing mobile spam

(1) Overview of the current situation and countermeasures

In Japan, it has become common to use mobile phones for sending and receiving Internet mail. Consequently, large volumes of spam were causing the same sort of problems frequently experienced with PC usage. Nevertheless, measures implemented using a multifaceted approach based on clearly defined cooperation between the public and private sectors have succeeded in dramatically reducing the amount of nuisance mail. As a result, nuisance mail sent from mobile phones in particular (including PHS phones) has declined to nearly zero.
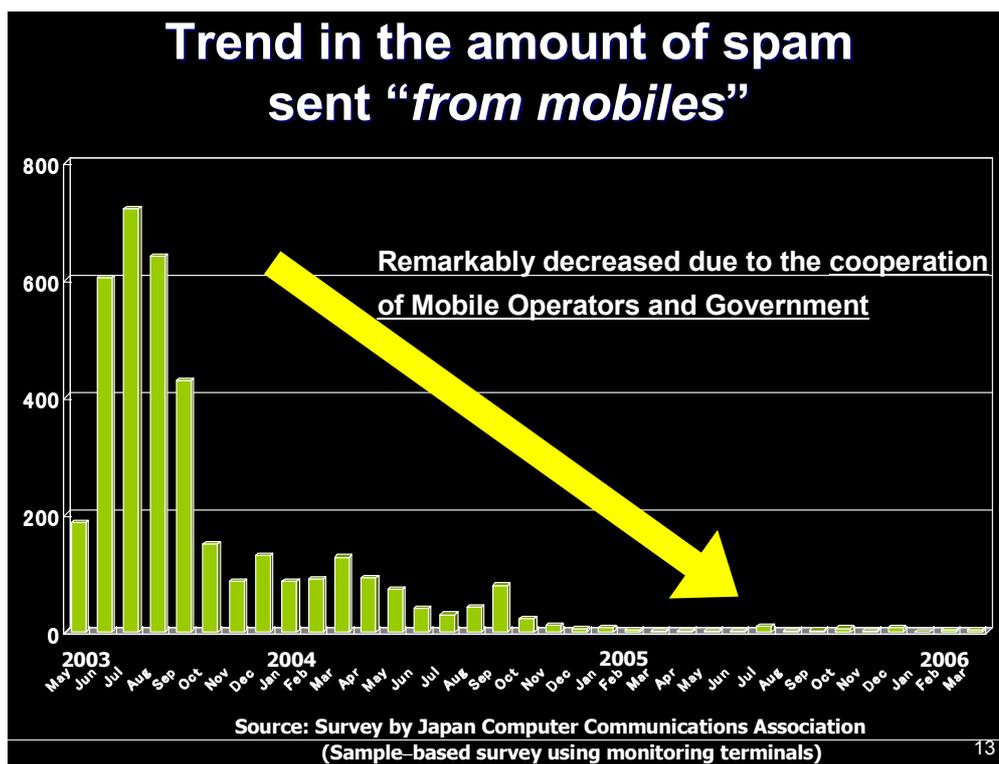
* From Japan's Measures against Spam(Telecommunications Bureau, Ministry of Internal Affairs and Communications, Japan)

The following is an overview[15] of the various measures that were taken by each sector.

i) Government

---

[15] For details, refer to the Final Report of the Study Group on a framework to handle spam of the Ministry of Internal Affairs and Communications (http://www.soumu.go.jp/s-news/2005/pdf/050722_2_02_00.pdf).

Nippon Keidanren (Japan Business Federation)

a. Implementing effective regulations against nuisance mail

- The Law on Regulation of Transmission of Specified Electronic Mail (the Anti-Spam Law) was passed (revised November 2005), establishing a sender's obligation[16] to indicate clearly in unsolicited mail that it is advertising. The law also prohibits the transmission of mail with fraudulent sender information (this applies to nearly 100% of nuisance mail) and sending mail under a fictitious address, among other measures.
- The law gave telecommunications carriers the right to deny service when a large volume of e-mail is sent at once was recognized as a measure against nuisance mail.
- As a result of this legislation, it became easier for the private sector to take action against nuisance mail.

b. Facilitation for establishing an information sharing system

- Sharing of information concerning parties that send nuisance mail is now recognized (with guidelines established with regard to the laws for the protection of privacy and personal information).
- In order to facilitate information sharing in the private sector, memoranda of understanding have been actively sought both multilaterally and bilaterally.

ii) Private sector
a. Information sharing

- As a measure against "migration,"[17] information is being shared concerning malicious operators in cases where contracts have been canceled.

b. Introducing the latest technologies

- As a technical solution, many ISPs are considering implementing sender domain authentication and Port 25 blocking, while the major ISPs have already taken these steps. These measures are proving effective as a measure against nuisance mail with spurious sending addresses.

c. Measures specific to mobile phones

- Since it is possible to restrict the users of mobile phones, operators place restrictions on permitted quantities of outgoing mail.[18]

d. Filtering

- Operators provide powerful filtering functions such as those that can be set to receive only from specified addresses.

iii) Private sector and government cooperation

---

[16] Two incidents were detected in the first half of 2006.
[17] Continuing to send spam using a different ISP from one that canceled a contract.
[18] The main mobile phone companies in Japan restrict the number of transmissions per account to several hundred to one thousand per day.
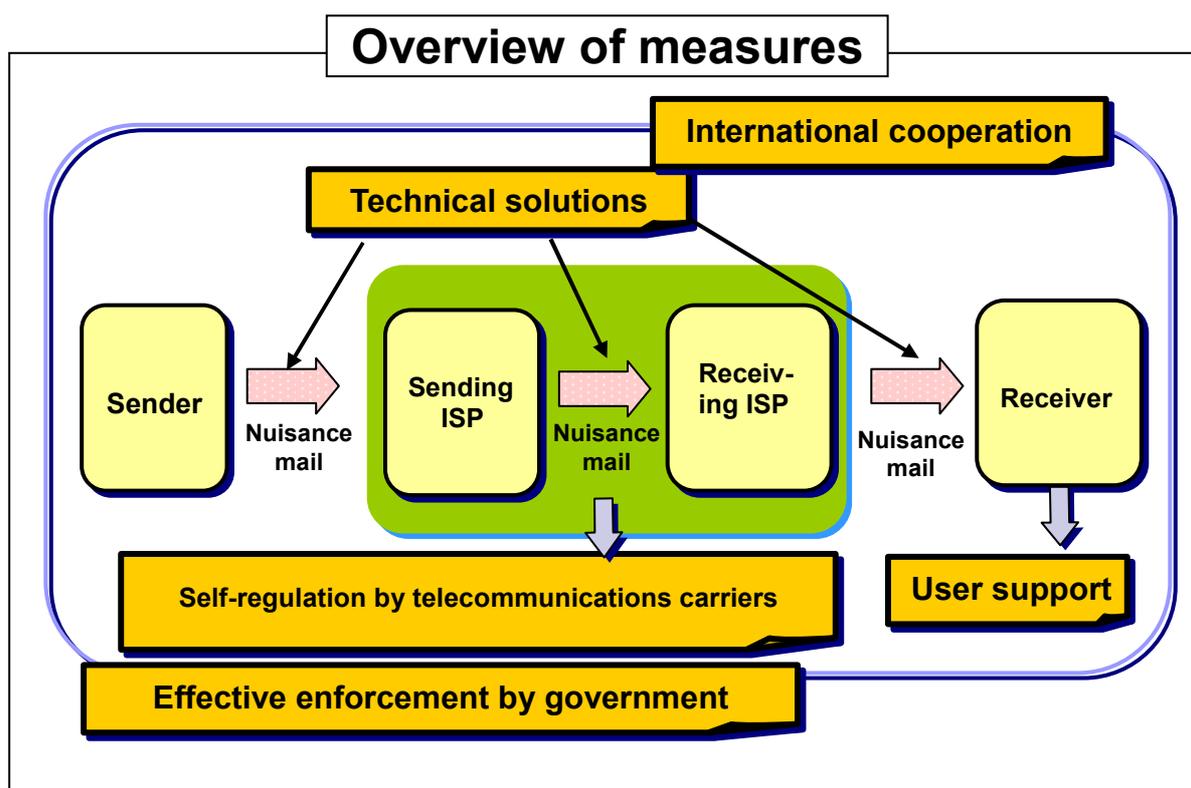
a. The government and private sectors are cooperating in a project to support the elimination of nuisance mail,[19] clearly establishing an official stance on anti-spam measures (from February 2005).

b. Awareness-raising activities
- Recommending the use of complicated e-mail addresses

(2) Issues for the future

The measures against spam sent from PCs are still insufficient, and looking to the future, we must work to establish an effective response through international cooperation. In particular it is important to build a framework for sharing blacklists on an international basis, as well as promoting worldwide cooperation in implementing a variety of technical countermeasures. Now it is necessary to take the discussion further concerning effective measures that combine technical and institutional measures, with reference to the anti-spam proposals of the OECD, MAAWG[20] (Messaging Anti-Abuse Working Group), JEAG[21] (Japan E-mail Anti Abuse Group) and other organizations.

Overview of measures

International cooperation

Technical solutions

| Sender | Nuisance mail → | Sending ISP | Nuisance mail → | Receiving ISP | Nuisance mail → | Receiver |

Self-regulation by telecommunications carriers

User support

Effective enforcement by government

* From the Final Report of the Study Group on a framework to handle spam of the Ministry of Internal Affairs and Communications

---

[19] The framework of the project is as follows: (1) The Nippon Information Communications Association analyzes nuisance mail received by a monitor function, and after identifying the sending ISP, reports it to the Ministry of Internal Affairs and Communications. (2) The Ministry recognizes the mail as unlawful and informs the ISP. (3) The ISP implements measures to halt use.
[20] http://www.maawg.org/home
[21] http://jeag.jp/

2. The threat of P2P file sharing software

(1) Overview of the current situation and countermeasures

As a result of flat-rate, always-on, high-speed broadband access becoming commonplace in Japan thanks to the nation's IT policies and strategic priority investment by the industry, P2P file sharing software applications that work well with broadband, such as Winny and Share, have gained broad popularity.[22] However, if these types of software designed for file sharing become infected with a particular virus, it can directly result in serious, unforeseen information leaks,[23] and there have been many cases in which users have not been sufficiently cognizant of this risk. As a result, there has been continuing leakage of various types of data in Japan caused by file sharing software. Although this is now recognized as a social issue, no solution to the problem has yet been found.

i) Main information leak incidents in 2006*

Date	Field	Type of information
August 2006	Critical infrastructure	Documents concerning piping in a nuclear power station
March 2006	Local authority	Resident registration information (personal data concerning 642 persons)
March 2006	Police	Personal data (including the real names of crime victims)
February 2006	Maritime Self-Defense Force	Documents concerning the Self-Defense Forces (including classified information)
January 2006	Hospital	Patient information

* A large number of leaks of private information have occurred in addition to these incidents.

ii) Responses to compounding factors

Although the direct cause of information leaks due to file sharing software is infection by an "exposure virus" such as the Antinny virus, there are several other contributory factors that are closely involved. The measures that were taken in response to the main factors are summarized below.

a. Technology-based measures

Firstly, as a technical fix for the virus that enabled malignant use of the file sharing software functions, the developer and other parties have provided a patch file to eliminate the vulnerability in the software, and software vendors have also provided tools for combating the virus. However, the problem of a "Zero-day attack"[24] when a new vulnerability is found still remains, and it is not possible to install pattern files for all the subspecies of viruses that are generated daily. For this reason there have been cases in which functions were provided that restrict the use of P2P file sharing software at the ISP as an emergency measure.

---

[22] As of July 2, 2006, the representative Winny software was being used on some 500,000 computers (according to research by NetAgent Co., Ltd.).

[23] File sharing software normally only has access to files in a specific location intended for sharing. However, when the software is infected with an "exposure virus," other locations can be accessed for sharing, leading to unforeseen leaks of information.

[24] Attacks that exploit a security vulnerability discovered in software before it is announced officially.

At the same time, studies are being undertaken concerning possible retroactive measures for when leaks occur on P2P networks, but so far they have produced no significant results.

Moreover the producer of Winny has stopped offering revisions and updates of the software[25] and so if a new vulnerability is discovered, there will no longer be an appropriate update to cover it.

b. Legal and institutional measures

In areas that cannot be covered by technology-based measures, the ability to respond with legal and institutional measures is being enhanced.

Businesses and governmental agencies are initiating restrictions on access to critical information assets using systemic and personnel criteria. At the same time, they are establishing security policies that do not permit this kind of information to be taken outside the organization, nor permit it to be used on computers for personal use that are not secured at an equal or higher level than those within the organization. All staff is required to comply with these regulations. With regard to personal data in particular, with enforcement of the Act on the Protection of Personal Information from April 2005, legal measures against leaks are being implemented. However, there are still organizations that are not in full compliance, whether due to insufficient understanding of the importance of security, or because the policy is unsuited to actual conditions and other reasons. In these organizations, leaks are still occurring through P2P file sharing software.

There are no laws regulating the use of P2P file sharing software by individuals or laws that obligate individuals to take antivirus measures, and countermeasures in this category have generally not been adopted.

c. Educational measures

In order for technology-based and legal measures to succeed, users must know enough about security and have the requisite skills, and in this regard, education is an important security measure. Many businesses and governmental agencies are training their staff in security, but there are many cases where the level of education is not sufficient.

In March 2005, the Chief Cabinet Secretary issued a comment about the risks of Winny regarding individual users, and the media are also working to raise awareness of the issue. However, with the spread of flat-rate broadband, users who are continuously connected to the Internet are on the rise, while media attention has raised the profile of Winny. In this situation where there is a great mass of general users, it is extremely difficult to implement educational and consciousness-raising measures that reach everyone. In addition, when leaked, highly confidential information is then posted on bulletin boards, it is dispersed even further afield.

Focusing too closely on data leaks alone has created the widespread but false impression that P2P file sharing software is simply a bad thing, and there is still insufficient understanding

---

[25] Arrested on suspicion of abetting breaches of the Copyright Act, the developer has pledged not to make any further improvements to Winny.

Nippon Keidanren (Japan Business Federation)

among users of the basic safeguards: avoid keeping important information assets on a PC with file sharing software installed on it, and take every possible security measure for the PC.

(2) Issues for the future

Among P2P file sharing software, Winny in particular has gained recognition as a social issue. The reason for this is that, while use of Napster and Gnutella resulted only in copyright infringements, with Winny, loss of information related to privacy and even national secrets also became a threat. What brought about this troubling state of affairs was the complex interaction of causes noted above, while the inability to take prompt and effective countermeasures was also a significant factor. At the IGF, we must consider more profoundly our stance on measures for the future, through discussion among all the parties concerned.

Furthermore, security risks arising from these combined factors are likely to propagate through ICT and new technological developments, which are appearing in various forms in all sorts of places around the world. Bearing these precedents in mind, we must now undertake in-depth discussion with the participation of all the stakeholders in preparation to address these new kinds of risk.

About Nippon Keidanren (Japan Business Federation)

Nippon Keidanren (Japan Business Federation) is a comprehensive economic organization born in May 2002 by amalgamation of Keidanren (Japan Federation of Economic Organizations) and Nikkeiren (Japan Federation of Employers' Associations). Its membership of 1,662 is comprised of 1,351 companies, 130 industrial associations, and 47 regional economic organizations (as of June 20, 2006).

The mission of Nippon Keidanren is to accelerate growth of Japan's and world economy and to strengthen the corporations to create additional value to transform Japanese economy into one that is sustainable and driven by the private sector, by encouraging the idea of individuals and local communities.

Nippon Keidanren, for this purpose, shall establish timely consensus and work towards resolution of a variety of issues concerning Japanese business community, including economic, industrial, social, and labor. Meanwhile, it will communicate with its stakeholders including political leaders, administrators, labor unions, and citizens at large. It will urge its members to adhere to Charter of Corporate Behavior and Global Environment Charter, in order to recover public confidence in businesses. It will also attempt to resolve international problems and to deepen economic relations with other countries through policy dialogue with governments, business groups and concerned international organizations.

Nippon Keidanren

Keidanren Kaikan, 1-9-4, Otemachi, Chiyoda-ku, Tokyo 100-8188
Email joho@keidanren.or.jp