

Nippon Keidanren's Position

1. Critical Internet Resources

The internet functions effectively under the current system. Further, despite a number of emerging issues, which are a natural outcome of continued growth, we believe the internet is developing healthily. An important reason for this is that the private sector, which is able to respond flexibly to technological developments and environmental changes, is responsible for internet operations and management. If this system was replaced by one in which an international organization guided by national governments took over internet management and operations, we believe it is possible that the internet would cease to function effectively, as the interests of national governments would inhibit quick decision-making. This would have a negative impact on civil society and business. For this reason, we strongly believe the current system of internet management and operations should be maintained.

On the other hand, as ICANN is under MOU with the government of the United States presently, we believe it is necessary to continue debate amongst stakeholders over how to increase neutrality and promote the global management of internet. However, it should be noted that IGF has no oversight function.

2. Access

Ongoing technological support for infrastructure development in developing countries is indispensable to bridging the digital divide. In particular, in agricultural areas, and other areas in which infrastructure remains inadequate, it is necessary to work to provide opportunities for access by building internet terminals in public spaces within communities. Further, as well as infrastructure development, it is important to educate and enlighten users how to utilize the internet appropriately. Developed countries should provide assistance in the form of human resources, educational materials, technical know-how and so on.

3. Openness

Respecting the right of open access to the internet, and the right to freedom of expression and debate, are above all else indispensable to the development of internet society. We believe that government regulations should be applied against illegal content, such as materials that constitute copyright infringement or violate privacy. However, regulations against harmful content, which include obscene content, should not be applied by government only, but rather should rely on self-regulation by the private sector.

Filtering is one concrete method of self-regulation. Although a certain degree of filtering is technologically feasible, and in fact some fee paying and free filtering software applications are available, user usage rates remain low. Businesses offering filtering services should work to upgrade their filtering technology, and should also work to further educate users.

Self-regulation by internet providers is also an effective method for eliminating harmful content. In Japan, self-regulation by internet providers is encouraged through law, striking an effective balance between the protection of copyright and privacy, and freedom of opinion and expression.

Using networks to pool the knowledge fosters new and creative endeavors. Since free utilization of artistic and literary works and mutual cooperation contribute to development of industry and culture, it is required to build the new balance between copy rights protection and promotion of practical use.

4. Security

The internet is the foundation of the information society, and realizing a secure internet environment in which anyone can use the internet safely is therefore an important task. However, end users continue to be infected by viruses from e-mail attachments of unknown origin, participate in criminal acts without their knowledge after being infected by BOTs, and so on. If user numbers continue to increase without being made aware of internet security issues, simply using the internet will increase the risk of infection. For this reason, it is urgent that we improve user awareness about internet security issues through educational campaigns.

National or regional efforts to respond to these problems are ineffective given that the internet is borderless, with cyber-crime commonly occurring across national borders. Further, if a single country or region is weak in its response it can become a haven for crime. For this reason, international society should share know-how and best practices related to internet security, and establish a system through a cooperative response framework can be developed.

Individual countries' CSIRT (Computer Security Incident Response Teams) currently share security information through FIRST (Forum of Incident and Security Teams), and we believe this is an effective framework for providing rapid notification of security incidents and for adopting measures against current and future threats. Countries or regions that do not have CSIRT should actively consider establishing a national CSIRT, and international organizations or developed countries should provide assistance in the form of human resources and know-how to these countries.

Further, in developing countries it is important not to neglect providing education on security issues in addition to providing opportunities for access and education about how to access the internet. Developed countries should therefore providing assistance promoting both "access" and "security" in tandem.

5. Diversity

Internationalized software applications and IDNs (internationalized domain names) should be developed in order to realize the society in which diversity of cultures and languages is respected and communications between internet users are encouraged further.

Towards the realization of society, in which the diversity of culture and a language is respected and communication among internet users is promoted, international support should be carried out further.

In addition, stakeholders should also meet to share technology and know-how designed to enable the elderly and people with disabilities to use the internet in a stress-free environment.