



# Communications News

Vol. 19 No. 15  
November 7, 2008

Biweekly Newsletter of the Ministry of Internal Affairs and Communications (MIC), Japan

ISSN 1349-7987

*Please feel free to use the articles in this publication, with proper credits.*

## STUDY GROUP REPORT

### Next-Generation Information Security Policies

#### Introduction - Changes in the Threats to Information Security -

In the first half of the 1990s, the majority of PCs were not connected to networks, and it was a time when system-based or file-based computer viruses proliferated through the use of external recording media such as floppy disks.

In the period from the second half of the 1990s through the first half of the 2000s, the usage environment progressed from LANs to the Internet, and the situation changed to viruses using the macro functions of word-processing or spreadsheet software, viruses attached to emails, and highly contagious viruses that exploited the vulnerability of software applications. The vast majority of these were untargeted attacks that were "fun crimes" showing off the attacker's interests and skills.

Starting a few years ago, these have changes to attacks with a clear money-related purpose, such as causing financial loss by targeting ICT functions at specific companies through attacks that disrupt services, or directing people to phishing sites via SPAM emails.

Recent trends have shown a move towards greater ingenuity and more sophistication in methods used to spread viruses,

and there have in particular been advances in the insidiousness of the attacks (making them more difficult to discern). For example, there have been cases such as fraudulent code being embedded into a legitimate site that has been attacked through its weaknesses, and viruses are then spread to those who visit the site from a PC that has a related vulnerability.

Attacks on information security will probably continue to gain in sophistication, and since, along with changes in environment, the information assets that are the target of this security will increase enormously, both in quality and quantity, taking countermeasures will become even more difficult.

Along with clarifying the issues that need to be addressed with ongoing countermeasures, MIC is envisaging a 3 to 5 year close future timeframe, and picking up the issues that are likely to arise from the changes in environment. In order to investigate the measures that should be taken for future information security, MIC set up the Study Group on Next-Generation Information Security Policies (chaired by Professor YASUDA Hiroshi of Tokyo Denki University) from October 2007, to conduct investigations for a period of 10 months. The group's findings are introduced here.

## CONTENTS

### STUDY GROUP REPORT

Next-Generation Information Security Policies	1
---	---

**International Policy Division,  
Global ICT Strategy Bureau  
Ministry of Internal Affairs and  
Communications (MIC)**  
1-2, Kasumigaseki 2-chome, Chiyoda-ku, Tokyo 100-8926, Japan  
Fax: +81-3-5253-5924  
Tel: +81-3-5253-5920

**We welcome your comments via:**  
[http://www.soumu.go.jp/joho\\_tsusin/eng/contact.html](http://www.soumu.go.jp/joho_tsusin/eng/contact.html)

**MIC Communications News is available at:**  
[http://www.soumu.go.jp/joho\\_tsusin/eng/newsletter.html](http://www.soumu.go.jp/joho_tsusin/eng/newsletter.html)

**Presentation materials of MIC are available at:**  
[http://www.soumu.go.jp/joho\\_tsusin/eng/presentation.html](http://www.soumu.go.jp/joho_tsusin/eng/presentation.html)

E-mail distribution of this newsletter is possible if desired.

## Threats on Information Security

### Current status of threat

The study group ascertained the current status of threats to information security as shown below.

(1) Threats from bot and other malware (threats from worm-type contagious viruses)

Bot is malicious software that is built with the purpose of causing harm to computers, so that the attacker can then manipulate the computer that has been attacked via the Internet. The damages caused can include stealing information from the computer, displaying fraudulent phishing sites, generating SPAM emails, acting as springboards for attacks on services, or spreading further bots.

(2) Threats through the use of social engineering (so as to circulate malware aimed at weaknesses and blind spots in people's actions and movements and steal information)

A typical example of this would be phishing, whereby emails are sent masquerading as financial institutions to obtain people's addresses, names, account numbers and credit card numbers,

and this has already caused a great deal of damage worldwide. More recently, spear phishing scams have begun to appear. At first sight, these look like perfectly ordinary emails, but information on senders has been camouflaged and the text has been customized so as to draw attention to a particular corporation or organization.

(3) External threats (unauthorized access from the outside, natural disasters etc.) and internal threats (human-error caused misses, intentional acts etc.)

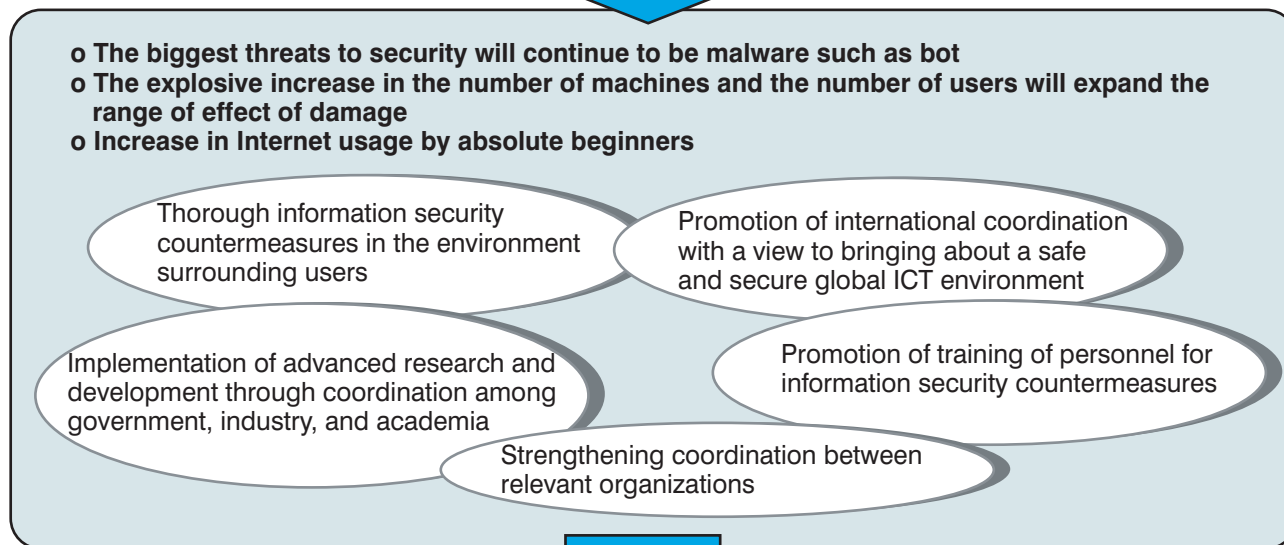
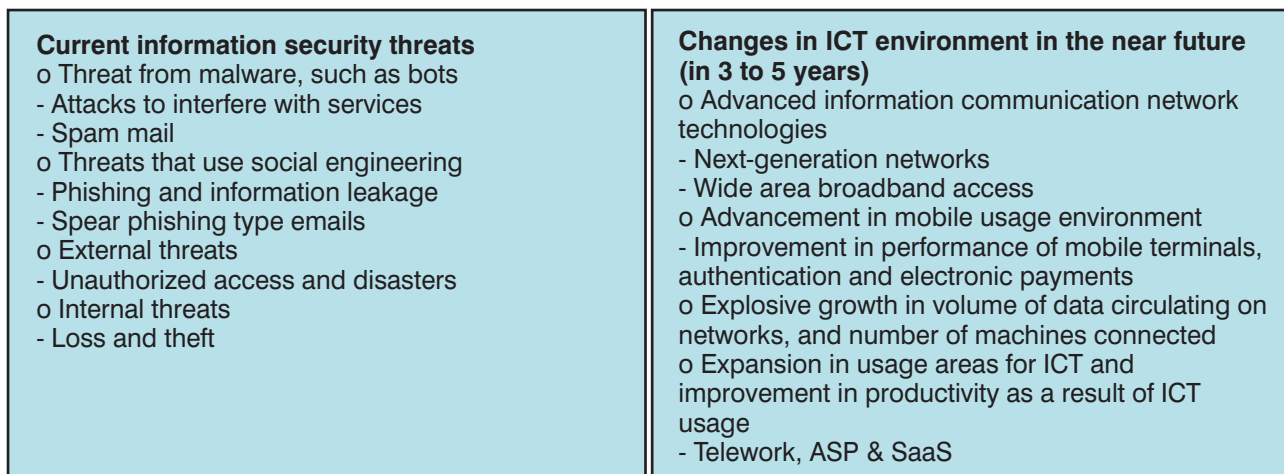
Countermeasures have mainly been sought from corporations, and the ongoing implementation and improvement of countermeasures is sought in the future. In particular, there have been a series of incidents of information leakage from loss, leaving machines behind or employees' home PCs that have been infected with viruses, so that, in addition to preliminary countermeasures, the implementation of after-the-fact countermeasures to prevent the spread of the damage and reduce it is being sought.

With regard to individuals, there is likely to be an increase in absolute beginners with neither awareness of information security

countermeasures nor skills, with the increase in usage by people with little experience of the Internet, the higher performance of information communication equipment and the diversification of information communications services.

### Changes and threats in the ICT environment in the near future

In the near future, along with next-generation networks, wide area wireless access, and further improvements in information communications networks, it is likely that the usage environment for mobile terminals will also expand to include authentication and electronic payments and the like. As a result, it is expected that the ICT usage framework will expand as ASP, SaaS, telework, and electronic money will become widespread, productivity will improve as a result of ICT and there will be changes in consumer activity. Since it is expected that, in conjunction with the changes in the ICT environment, there will be explosive growth both in quality and quantity of the information assets that need to be secured, which will make countermeasures even more difficult than they have been to date.



**Vitalization and streamlining of socio-economic activities through greater use of ICT, and increasing international competitiveness**

## Next-Generation Information Security Policies

The study group makes the following proposals to address the information security threats described above, to vitalize and streamline Japan's socio-economic activities further through the use of ICT, and to bring about a strengthening of international competitiveness.

It is necessary that users are strongly aware that, when they are affected by malware such as bot, it is not just them who suffers the consequences as it is possible that, without their even being aware of it, they are in turn causing harm to others, and in order to work towards thorough information security countermeasures when using the Internet, the government needs to implement much greater information initiatives, in coordination with relevant organizations.

In addition, since elementary and junior high school children use the Internet and mobile phones, it is necessary to work towards implementing more positively than to date measures for ICT media literacy so that children can use the

services safely and securely, in the same way as they learn to follow traffic regulations, rather than just using high performance information communications equipment and services.

At the same time, in order to improve information security for society as a whole, it will be necessary for everyone concerned, including telecommunications operators, service providers, information communication equipment manufacturers and resellers, and information security businesses, to join together in putting in place a system for ongoing cross-industry investigation concerning issues relating to information security and countermeasures.

### Conclusion

The study group envisioned the issues that need to be given priority on an ongoing base, as well as the future 3 to 5 years ahead and organized and classified issues that will arise as a result of changes in the environment, including the transitory process. ICT will continue to grow more sophisticated and information communications services will become more

diversified, and there is the fear that new threats and issues will arise which have not yet been anticipated. In order to respond in a timely and appropriate fashion to a state of affairs that will continue to grow more complicated, we strongly recommend that all the principal concerned organizations coordinate their efforts in implementing countermeasures.

MIC has put in place bot countermeasures in coordination with METI, at the Cyber Clean Center (<http://www.ccc.go.jp>). Aside from providing the warning system and clean-up tools for users of PCs that have been infected with bots, it is also implementing information and warning activities concerning measures for avoiding infection by viruses. Also, MIC's information security site ([http://www.soumu.go.jp/joho\\_tsusin/security/index.htm](http://www.soumu.go.jp/joho_tsusin/security/index.htm)) is aimed at the general population and provides easy to understand contents about information security related knowledge and countermeasures.

MIC will continue in the future to promote the putting in place of a safe and secure ICT environment.