Opening Statement of Chairperson by Professor Ryozo Hayashi
At The ASEAN Japan Information Security Policy Meeting
October 10, 2012

Director, Meiji Institute for Global Affairs
Meiji University

(Global Economy)

Since The Lehman Shock in 2009, the world's economy has been sluggish. Prior to 2009, the world's financial markets had extended huge amounts of credit which created unsustainable asset bubbles. Eventually, these bubbles burst. Then, worldwide government fiscal stimulus packages, taken as a countermeasure, only produce a new vulnerability: excessive government debt. No fundamental solution to these problems is in sight.

Among major economies, Europe recorded negative growth this year and is expected to be weak in the coming couple of years. The US economy is slowing down due to low job growth which reduces demand. China, which has been a locomotive power of the global economy for the last couple of years has, because of weak exports to Europe, lowered her growth rate and has shown signs of reaching an inflection point. Many international organizations have negatively revised their forecast of growth rates of these economies.

So far, the Japanese economy has shown a solid recovery from the earthquake. However, a rapid yen appreciation, along with an uncertainty in energy policy, has started to erode the international competitiveness of Japanese companies. The ASEAN economy is not operating in an isolated environment, and careful economic management is required. In this context, Japanese direct investment into ASEAN countries increases in importance for both economies.

(Japanese Oversea Direct Investment)

Japanese direct investment to ASEAN countries has played an important role in maintaining the competitiveness of Japanese companies and in the development of ASEAN economies. Last year, that investment exceeded one trillion yen, which was doubled from the previous year, and ASEAN economies became the largest destination for Japanese investments. The increase is in qualitative terms too. In addition to traditional destinations such as Indonesia, Malaysia and Thailand, now the Philippines, Cambodia, Laos and Myanmar have become important recipient countries.

Such changes partly reflect the increase of labor costs in China. However, a more

important reason is the attractiveness of the region, first as a production center and secondly as a major consumer region. This successful development was brought about by the continuous deepening of the level of integration and the consequent balanced development of their economies.

This successful integration was made possible by institutional arrangements such as regional free trade agreements (AFTA), the enlarged economic partnership arrangement beyond ASEAN countries, and by the development of ICT infrastructures. Information infrastructure and information technologies play an important role in the development of business and production networks. They also contribute to the enhancement and performance of many institutions and infrastructures, which were critical for ASEAN economic development.

(Information Security Policy)

In order to protect such critical networks information security measures are indispensable. However, technological developments and the increasing dependency on cyber networks make this task more difficult and serious. Threats through or against networks have become   much more skillful, more organized and more difficult to detect, while the potential economic damages have increased enormously   and spread to the national security area.

The most serious threat is the spread and sophistication of "advanced persistent threats." They have a clear objective of confusing specific networks or to steal specific information. The malware is sent by e-mails and is crafted in such a deceptive manner that the receiver opens the mail without doubts. This approach is not easily caught by traditional antivirus software.   DDos attacks have scaled up too; groups of hackers who share common beliefs engage in large scale coordinated DDos attacks. These organized attacks against networks have become a common phenomenon.

The introduction of new devices, new technologies and new network environments invites new threats.   New smart phones have spread rapidly as internet devices. However, their operating systems are not well guarded against cyber attacks. Users are usually naïve about cyber threats. This makes the smart phone an easy target for hackers. Attacks against control systems, which operate important manufacturing facilities and critical infrastructures, are another big concern. The invasion of malware to control system is often reported. Historically, these systems had been isolated from networks,   are not prepared to protect themselves from cyber attack.   Now, "smart grids" or "smart communities" have come into being.   As they are introduced every

machine will be connected with every other machine without human interaction. Again, many of these machines are not designed to be connected with the internet. The development of information security measures is critical. The wide spread use of "cloud computing" also requires new types of countermeasures, because users usually cannot control developments at the time of an incident.

These new situations require new counter measures. In the case of APT, it is not enough to mend fences one by one as they are found. The target is the network as a whole. Security measures have to be comprehensive. It is certainly important to enhance the level of security of targeted organization, such as governments or corporation which runs critical infrastructures. In order to enhance the defensive capability of society against such attacks, there should be some mechanism for members to share their experiences. Because of the nature of targeted information or organizations, no victim likes to reveal the fact that they have been successfully attacked. There should be a neutral trusted third party to establish the essential facts and to convey their necessary essence to relevant parties.

In the case of new devices, users have to be alerted. It is urgent to raise incident analysis capability and to develop new and stronger operating systems. These new counter measures require human resources at various levels; capable researchers, engineers, security experts in user organizations, detective experts in governments and so forth.

(International Cooperation)
These counter measures can only be effective or more effectively taken through international cooperation. In many countries, the urgency of counter measures and the importance of international cooperation are recognized at the highest levels. These matters are discussed at Economic Summits, in the United Nation, at OECD and at special multinational forum such as the London conference last year. Various thoughts and experiences are exchanged towards simultaneously providing maximum security while maintaining the usefulness of the internet.

The Japan ASEAN Information Security Policy Meeting has successfully launched initiatives such as The "Information Security Awareness Program." We are ready to discuss many important reports and proposals this year. I am sure that we will continue to build on these achievements, and to be an important part of such international cooperative activities.