

## **Report from the Internet Monitoring (TALOT2)**

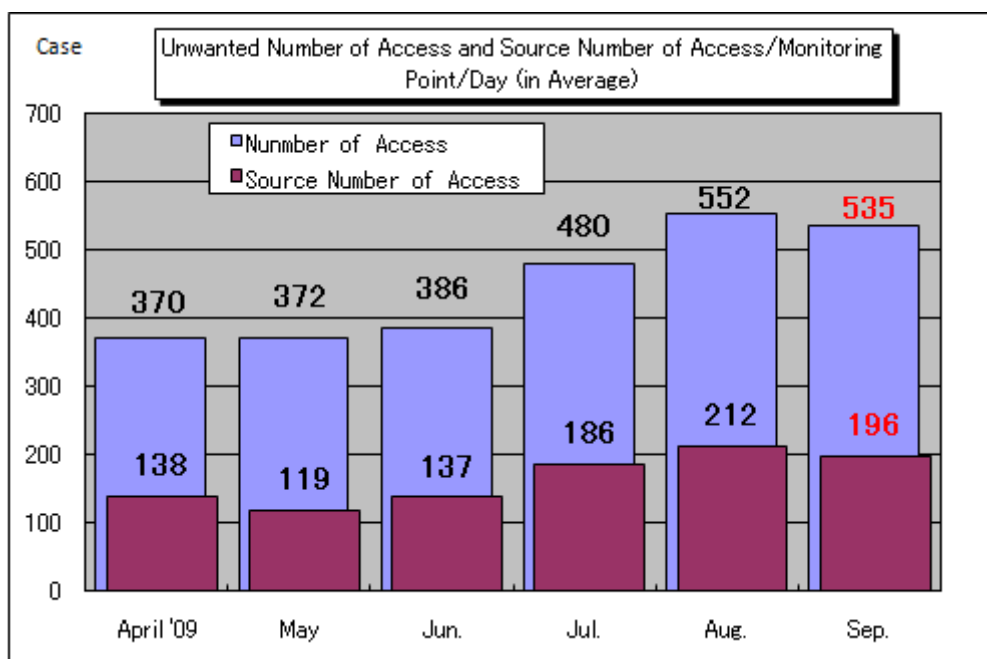
September 2009

### **1. To the General Internet Users**

In the Internet Monitoring (TALOT2), unwanted (one-sided) access in September totaled **160,487** cases for the 10 monitoring points and the gross number of the sources\* was **58,770**: unwanted (one-sided) access captured at one monitoring point was **535** accesses from **196** sources per day (see the Chart 1-1).

**Gross Number of Source (\*):** The gross number of the source accessed TALOT2. For your further information, the source is counted as 1 when accessed by the same source from the same day to the same point/port.

The environment for each monitoring point in TALOT2 is nearly equal to general users' Internet connection; it can be considered that the same amount of unwanted (one-sided) access may be received by the general internet users.



**Chart 1-1: Unwanted (One-sided) Number of Access and Source Number of Access/Monitoring Point/Day**

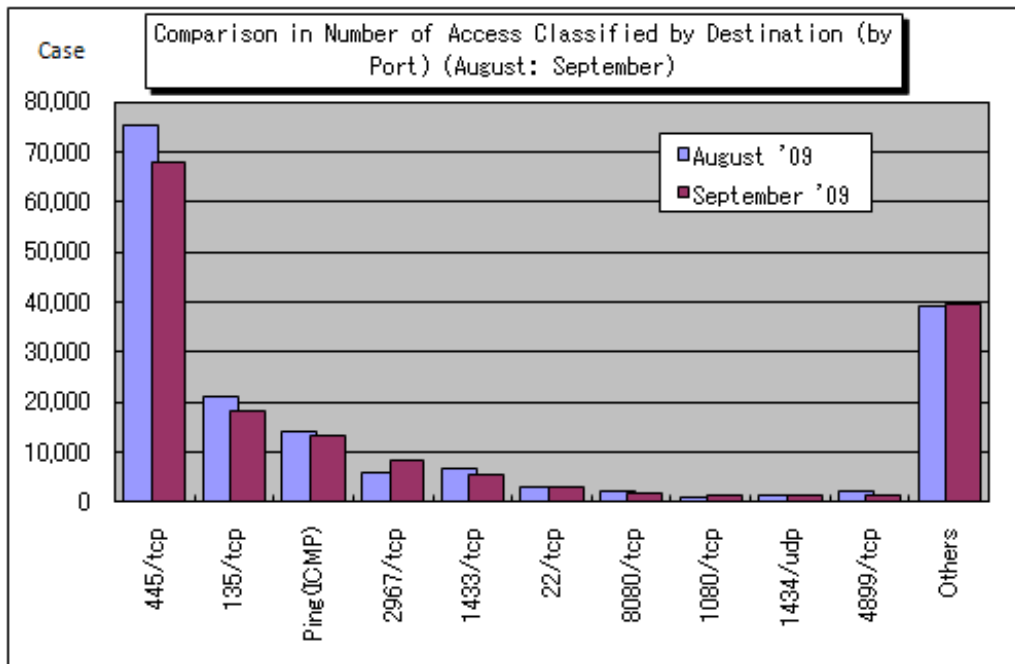
The Chart 1-1 shows the unwanted (one-sided) number of access (average) and the source number of access (average)/monitoring point/day from April to September 2009. Both the unwanted (one-sided) number of accesses were subtly decreased from the ones in August.

The Chart 1-2 shows the comparison in unwanted (one-sided) number of accesses classified by destination (by port) in August and September. There were none of the port from which/to which accesses drastically shifted. The access to the port 445/tcp which was continually increasing from 4 months ago was turned to decreasing from September.

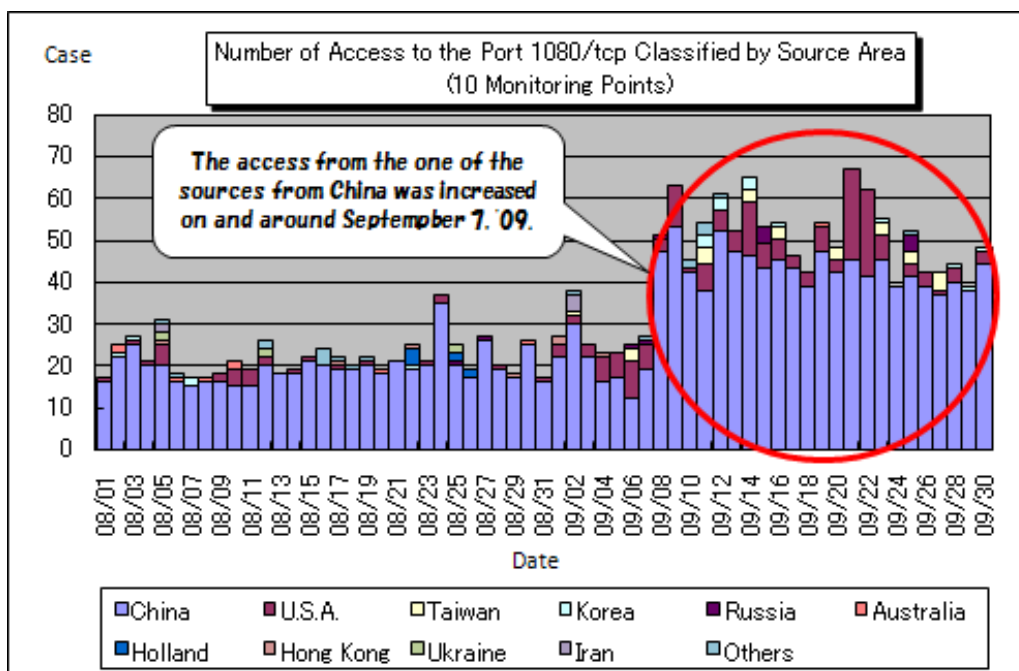
In addition, the access to the port 1080/tcp which never been listed in the one of frequently accessed ports could often be observed. This was the access from one of the sources in China for which access was continually observed from September 7 (please refer to the Chart 5-3): it could be realized that the same source accessing to the port 1025/tcp was also observed simultaneously. These accesses were monitored by of 7 monitoring points out of 10 in TALOT2 system; accordingly, it could be assumed that the same event may have been caused extensively (please refer to the Chart 5-4 and 5-5).

The reason why the source was continually accessed to these ports was unknown.

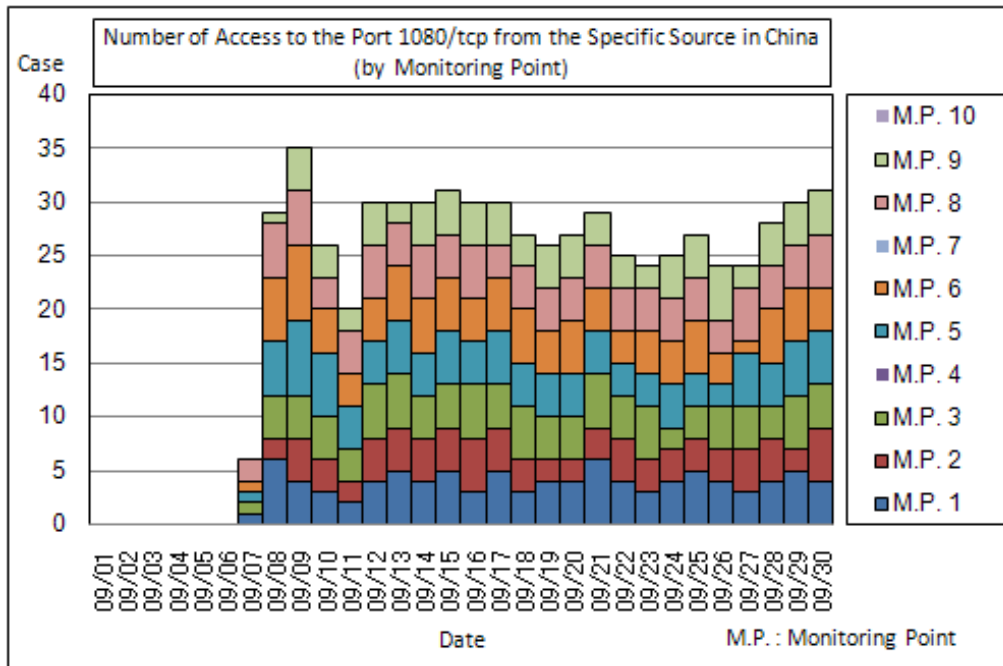
SOCKS server\*: the one of proxy servers which conducts communication to the Internet on behalf of corporate LAN, etc.



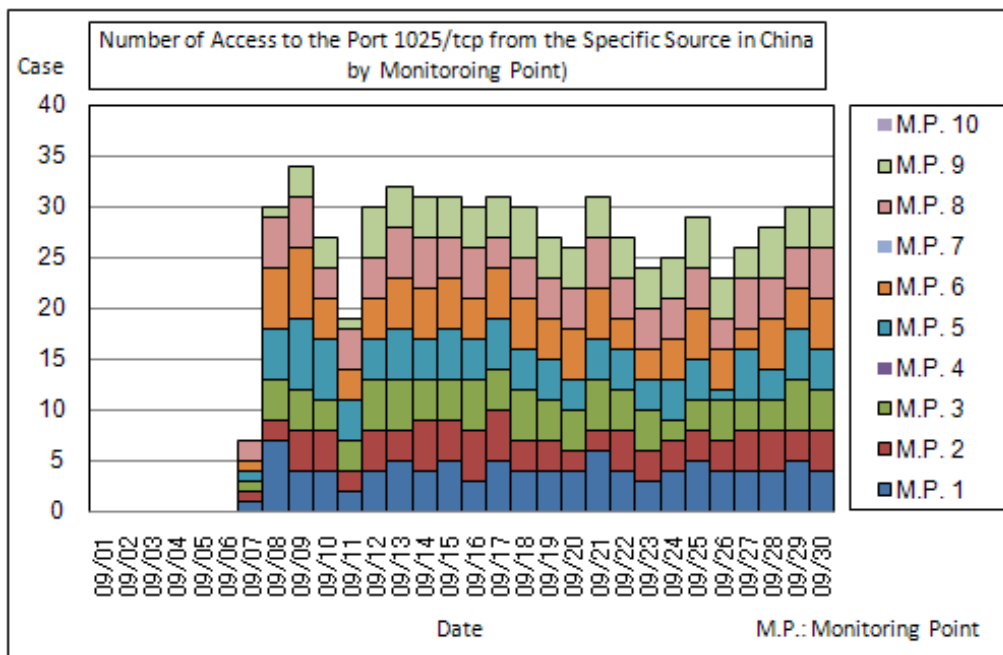
**Chart 1-2: Comparison in Number of Access Classified by Destination (by Port) (August: September)**



**Chart 1-3: Number of Access to the Port 1080/tcp Classified by Source Area (10 Monitoring Points Total)**



**Chart 1-4: Number of Access to the Port 1080/tcp from the Specific Port in China (by Monitoring Point)**

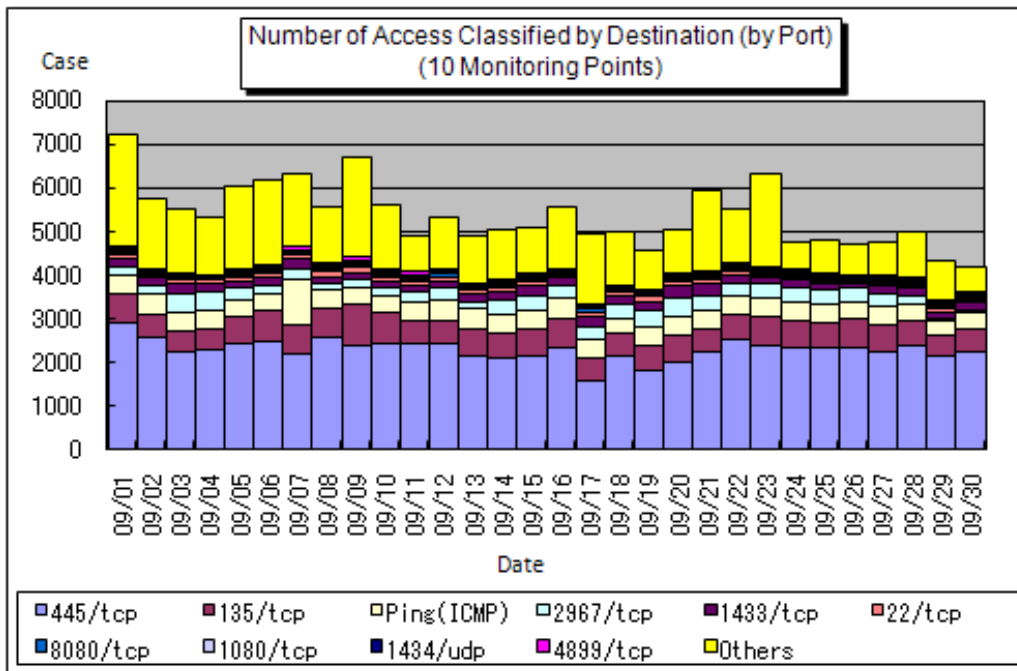


**Chart 1-5: Number of Access to the Port 1025/tcp from the Specific Port in China (by Monitoring Point)**

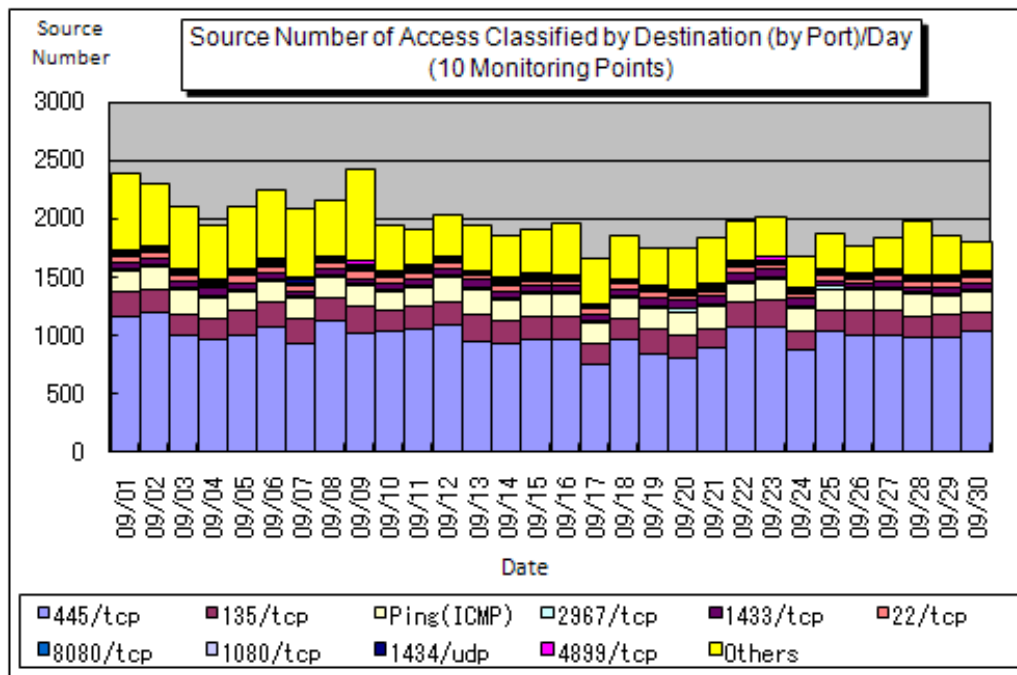
## 2. Unwanted (One-sided) Number of Access in September 2009

### (1) Accessing Status Classified by Destination (by Port)

The Chart 2-1 shows the unwanted (one-sided) accessing status (number of access) and the Chart 2-2 shows the unwanted (one-sided) accessing status (source number of access) in September 2009.



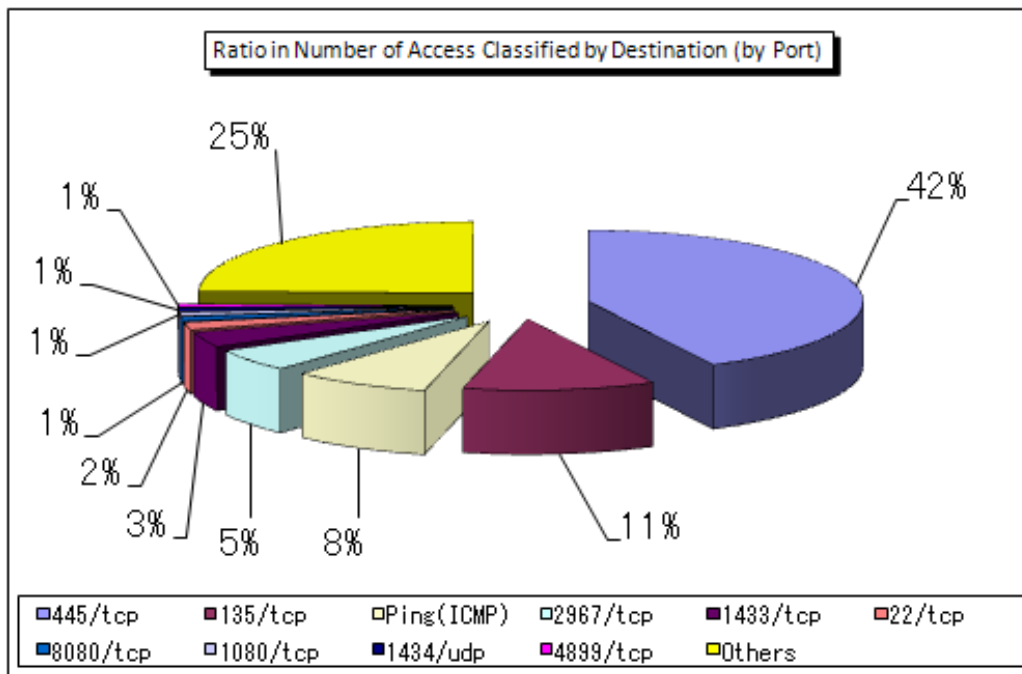
**Chart 2-1: Number of Access Classified by Destination (by Port)/Day in September 2009**



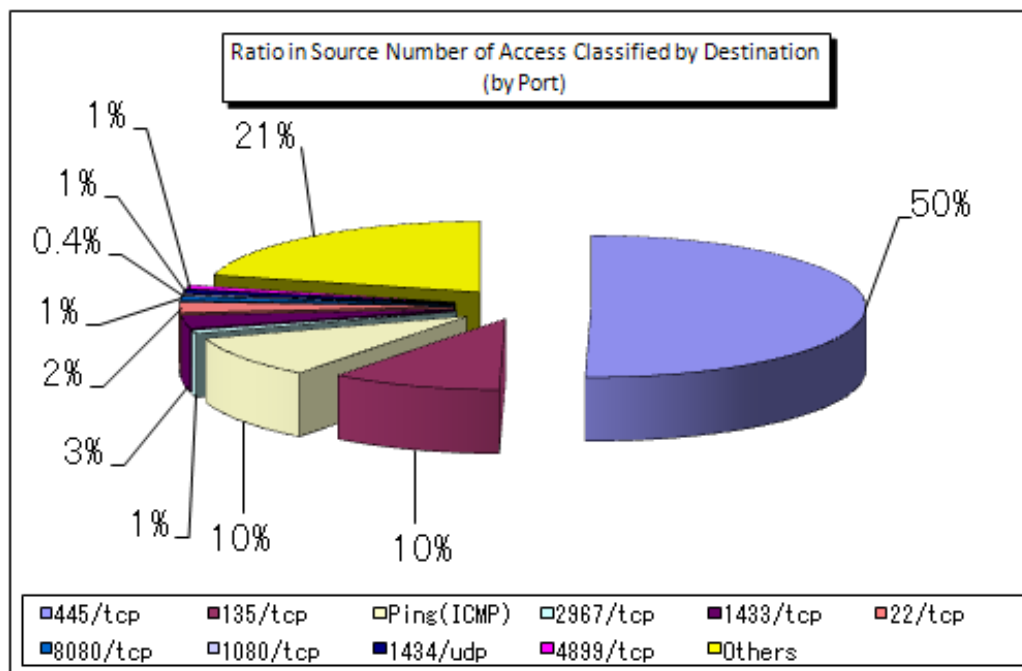
**Chart 2-2: Source Number of Access Classified by Destination (by Port)/Day in September 2009**

**(2) Ratio Classified by Destination (by Port)**

The Chart 2-3 shows the ratio in number of access classified by destination (by port) and the Chart 2-4 shows the ratio in source number of access classified by destination (by port) in September 2009. In addition, numbers in ratio are rounded at the 1<sup>st</sup> arithmetic point so that they may not make 100% sharp, accordingly.



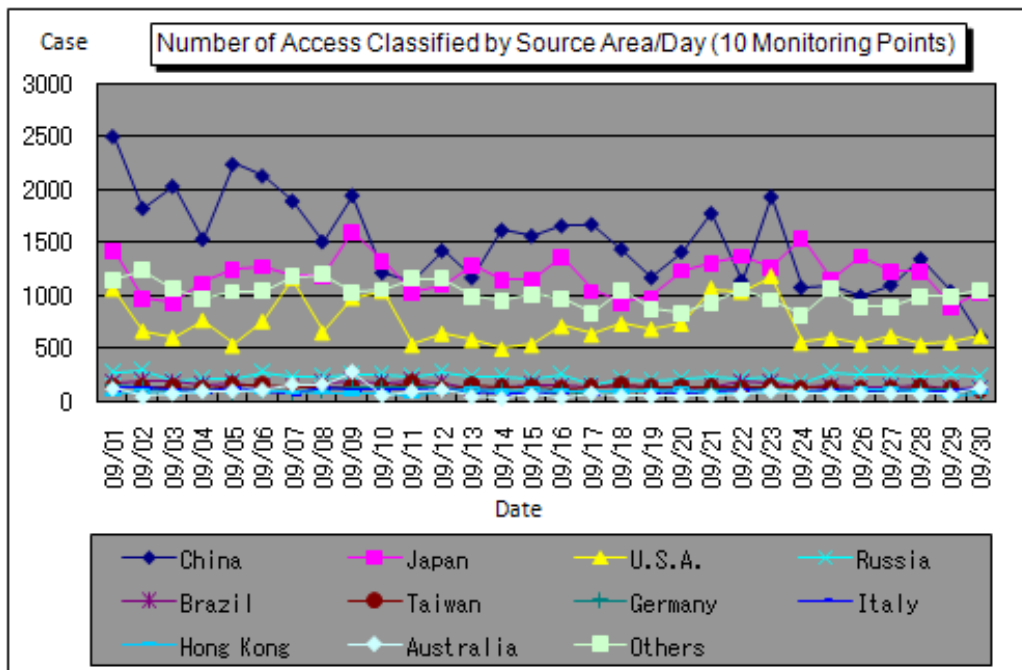
**Chart 2-3: Ratio in Number of Access Classified by Destination (by Port) in September 2009**



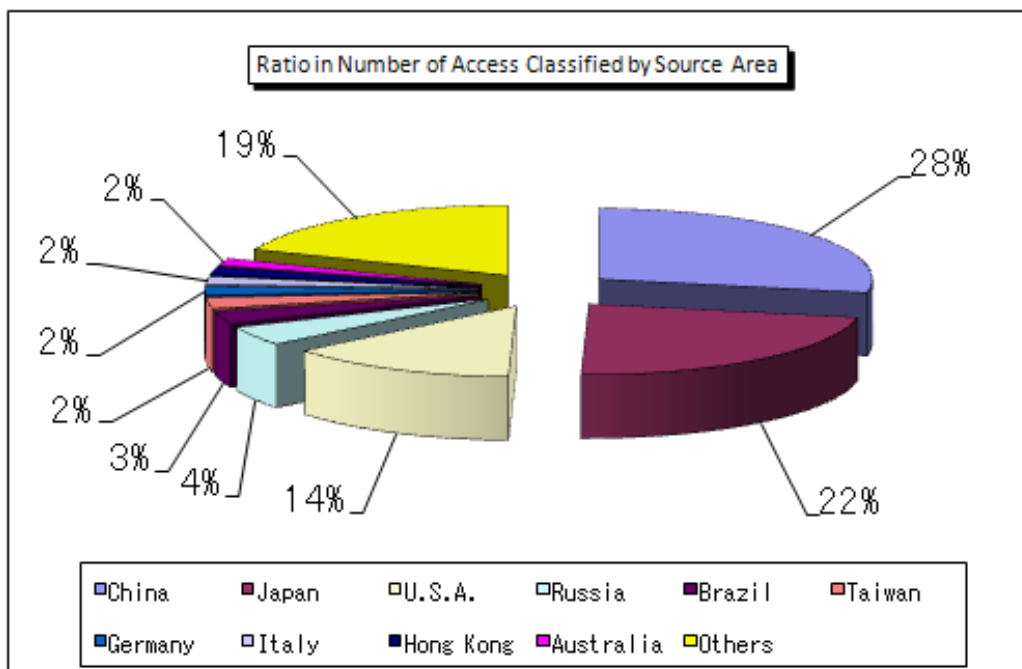
**Chart 2-4: Ratio in Source Number of Access Classified by Destination (by Port) in September 2009**

**(3) Accessing Status Classified by Source Area**

The Chart 2-5 shows the shift in number of access classified by source area and the Chart 2-6 shows the ratio in number of access classified by source area in September 2009. In addition, numbers in ratio are rounded at the 1<sup>st</sup> arithmetic point so that they may not make 100% sharp, accordingly.



**Chart 2-5: Number of Access Classified by Source Area/Day in September 2009**



**Chart 2-6: Ratio in Number of Access Classified by Source Area in September 2009**

The Chart 2-7 shows the shift in source number of access classified by source area and the Chart 2-8 shows the ratio in source number of access classified by source area in September 2009. In addition, numbers in ratio are rounded at the 1<sup>st</sup> arithmetic point so that they may not make 100% sharp, accordingly.

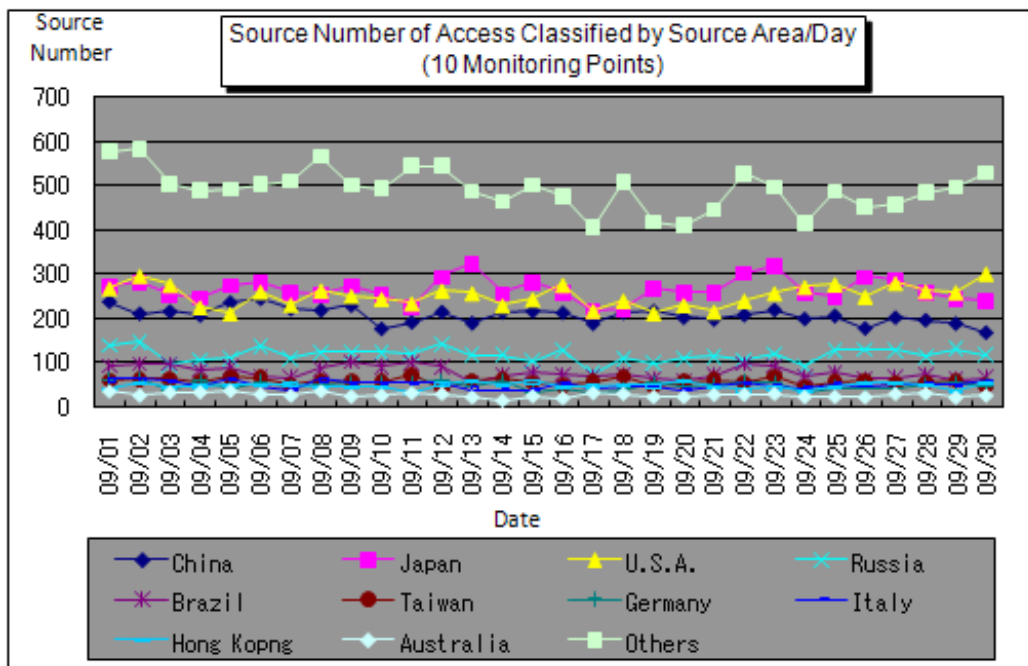


Chart 2-7: Source Number of Access Classified by Source Area/Day in September 2009

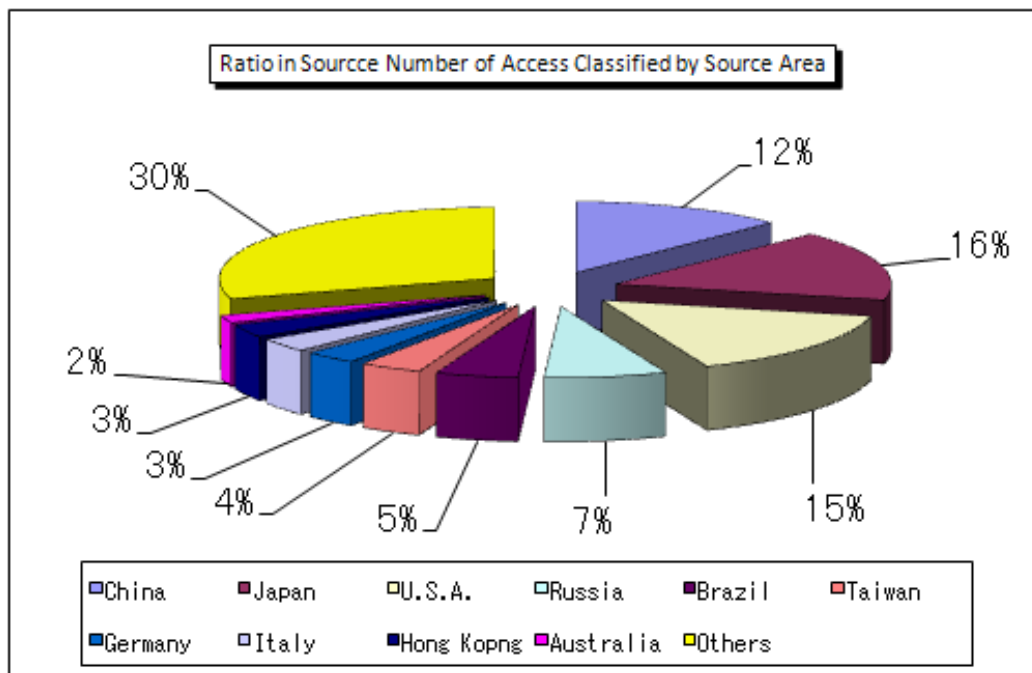
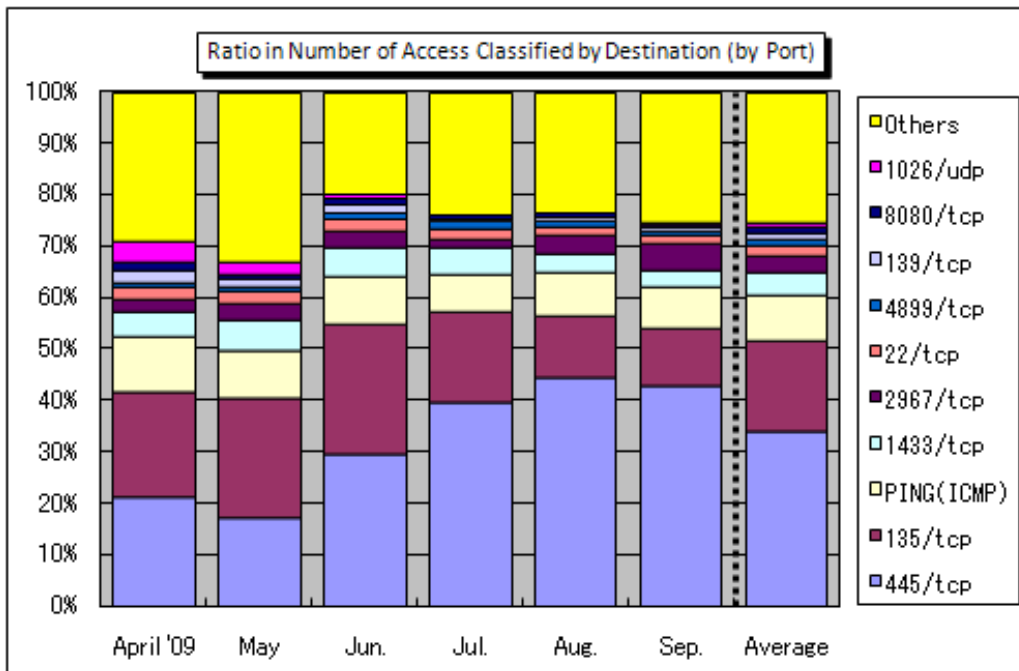


Chart 2-8: Ratio in Source Number of Access Classified by Source Area in September 2009

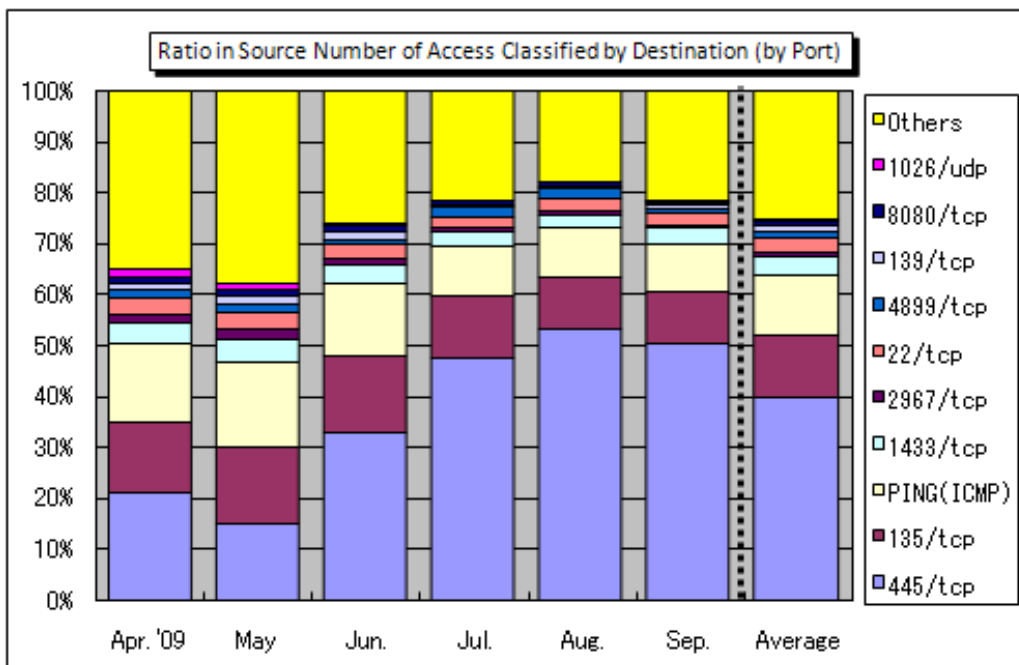
### 3. Statistical Information

#### (1) Ratio Classified by Destination (by Port)

Chart 3-1 shows the ratio in number of access classified by destination (by port) and the Chart 3-2 shows the ratio in source number of access classified by destination (by port) from April to September 2009.



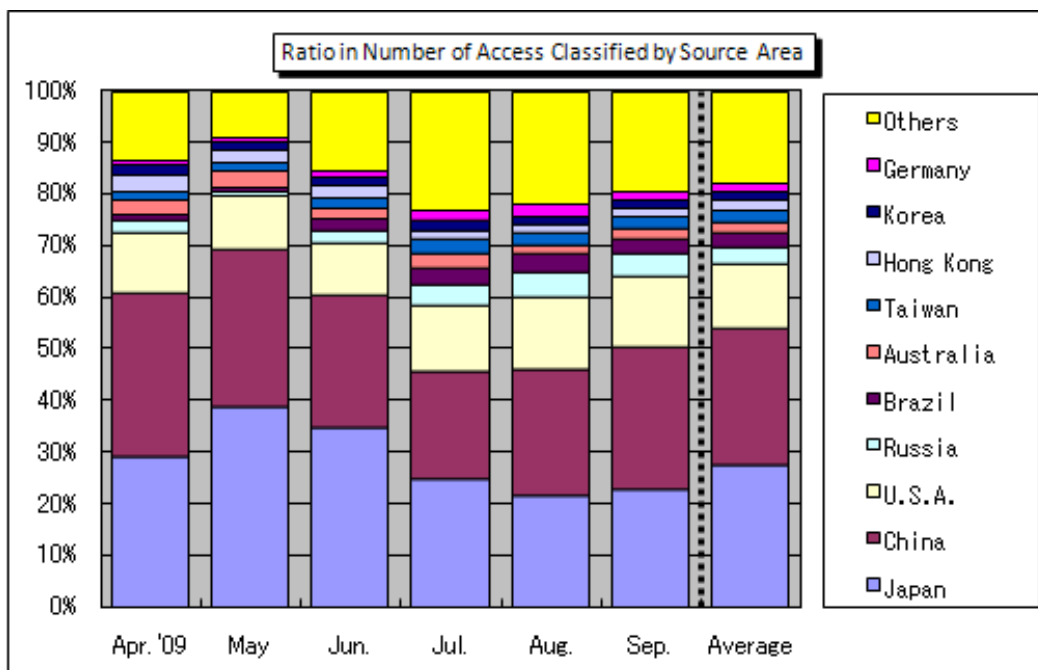
**Chart 3-1: Ratio in Number of Access Classified by Destination (by Port) from April to September 2009**



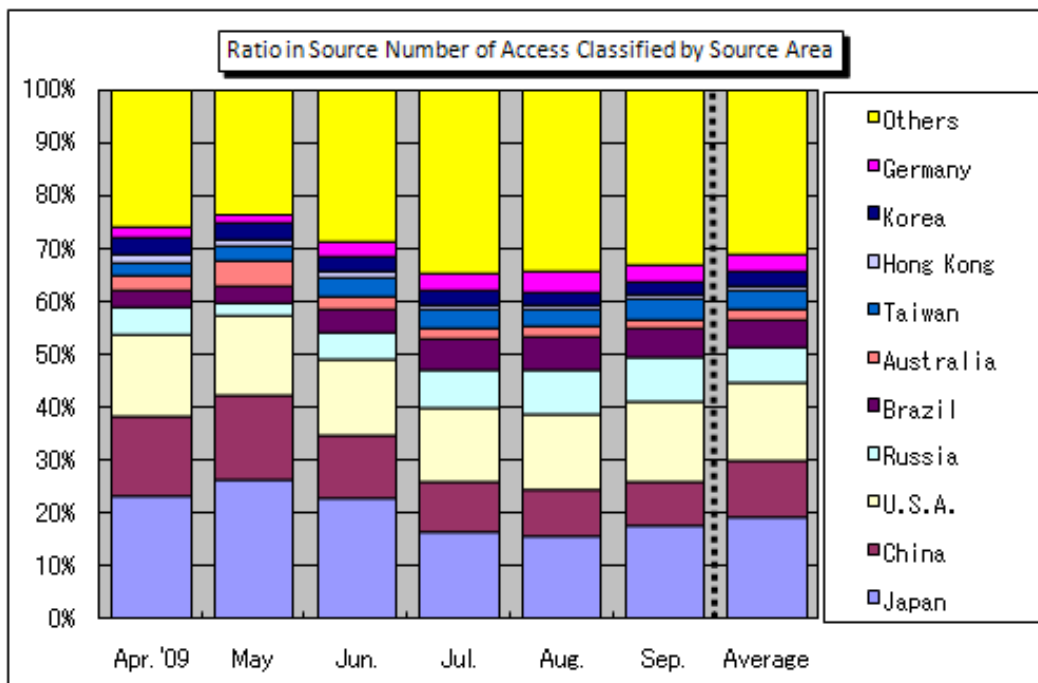
**Chart 3-2: Ratio in Source Number of Access Classified by Destination (by Port) from April to September 2009**

**(2) Ratio Classified by Source Area**

The Chart 3-3 shows the ratio in number of access classified by source area and the Chart 3-4 shows the ratio in source number of access classified by source area from April to September 2009.



**Chart 3-3: Ratio in Number of Access Classified by Source Area from April to September 2009**



**Chart 3-4: Ratio in Source Number of Access Classified by Source Area from April to September 2009**

#### 4. Supplementary Explanations

Following are the explanations for the destination (port type) remarkably accessed (either in-bound or out-bound or both) in September 2009.

<b>Port Type</b>	<b>Interpretations/Descriptions</b>
445/tcp	Renowned for those file sharing (network sharing) that has not been well-protected and unauthorized computer accesses (W32/Sasser, etc.) which targets vulnerabilities specifically in Windows 2000.
135/tcp	This is the default port for the Microsoft Windows Remote Procedure Call (RPC) and is renowned for the unauthorized computer accesses (W32/MSBlaster, etc.) which target vulnerability (MS03-026) relevant to RPC.
Ping (CMP)	This port is originally used to check if the other party or person's computer is in operation and is renowned for being exploited by W32/Welchia, etc. to search to target computers for unauthorized accesses.
2967/tcp	High potential of access which targets vulnerability in Symantec products such as Symantec Client Security and Symantec AntiVirus, etc.
1433/tcp	This is the default port for Microsoft SQL Servers which searches those computers for which SQL Server is in operation. The port is also renowned for unauthorized computer access activities which target vulnerabilities in SQL Servers.
22/tcp	The access which targets SSH (Secure Shell: the command execution tool for which security is enough strengthened by encrypting its communication path) to intrude to a system by password cracking attack.
8080/tcp	This is the frequently accessed port to connect to HTTP Proxy: it is probable that the port is exploited by malicious intent when he/she explores such proxy server (s) which is available to use the steppingstone to access fraudulently.
1080/tcp	This is the typical port used by the SOCKS server, the one of proxy servers, and is frequently accessed by malicious intent to probe such proxy server which is exploitable as a steppingstone server for fraudulent accesses.
1434/tcp	Renowned by unauthorized computer access targeting the vulnerability (by W32/SQL Slammer) in Microsoft SQL Server, etc.
4899/tcp	Renowned for such unauthorized computer access which targets to the vulnerability in RAdmin for remote operation (RAdmin is the application which enables to remotely operate multiple computers).

***Inquiries to:***

Information-Technology Promotion Agency, Security Center  
Ooura/Hanamura/Kagaya

Tel.: +81-3-5978-7527

Fax: +81-3-5978-7518

E-mail: [isec-info@ipa.go.jp](mailto:isec-info@ipa.go.jp)