

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

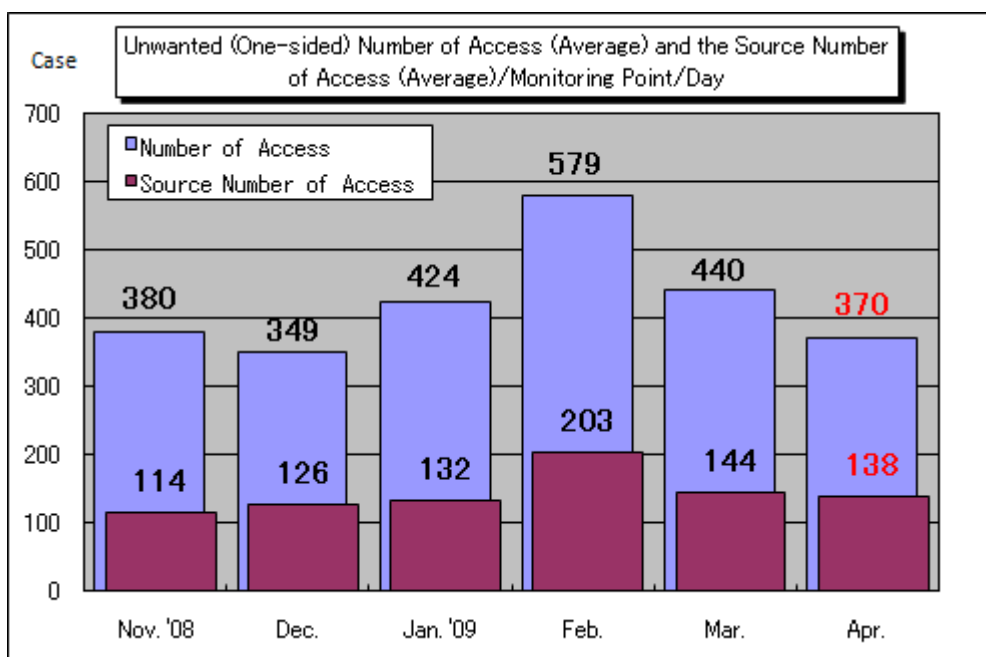
April 2009

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

In the Internet Monitoring (TALOT2), unwanted (one-sided) access in January totaled **110,995** cases for the 10 monitoring points and the gross number of the sources\* was **41,366**: unwanted (one-sided) access captured at one monitoring point was about **370** accesses from about **138** sources per day.

**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.

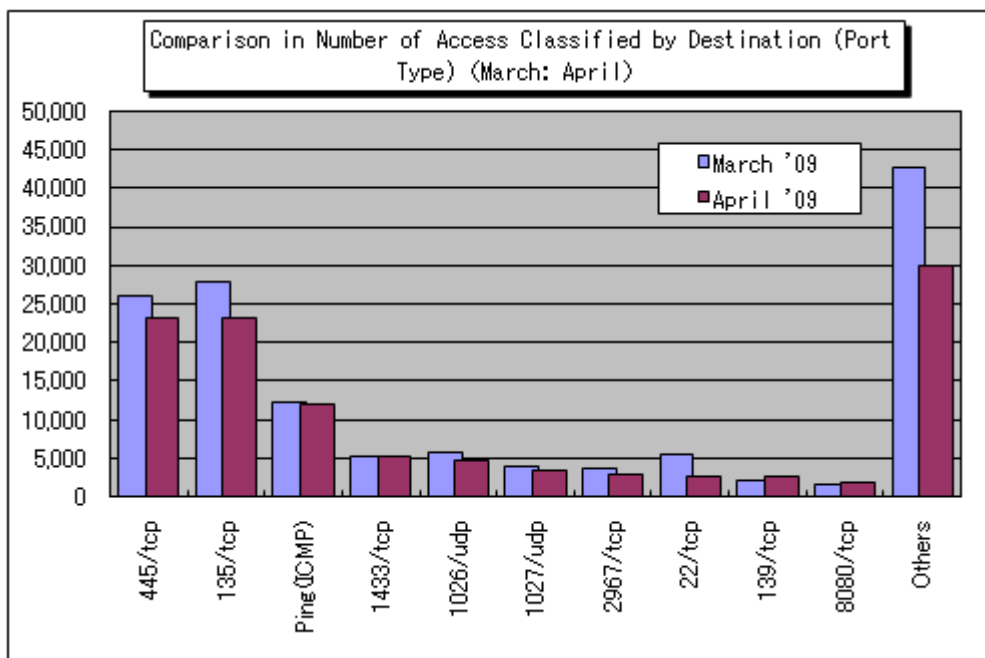


**Chart 1-1: unwanted (One-sided) Number of Access and Source Number of Access/Monitoring Point/Day**

Chart 1-1 shows the unwanted (one-sided) number of access and the source number of access/monitoring point/day from November 2008 to April 2009. Both the unwanted (one-sided) number of accesses were decreased from March.

The Chart 1-2 shows the comparison of number of accesses classified by destination (port type) in March and April.

None of the 10 frequently accessed ports was drastically shifted in number from March. The cause mostly affected the frequently accessed ports to decrease was the accesses to the ports other than the 10 frequently accessed ports: the number of access (average) lessened about 13T (decreased about 70%) from March. Another reason was that there observed several accesses for which cause was unknown in March: however, in April, such access was not observed.

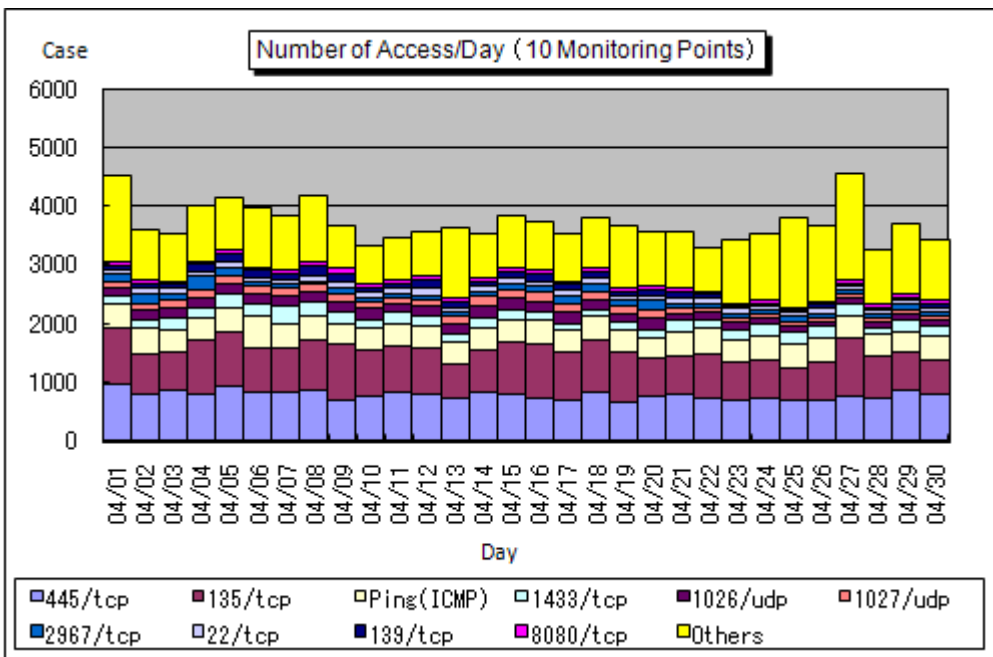


**Chart 1-2: Comparison in Number of Access Classified by Destination (Port Type) (March: April)**

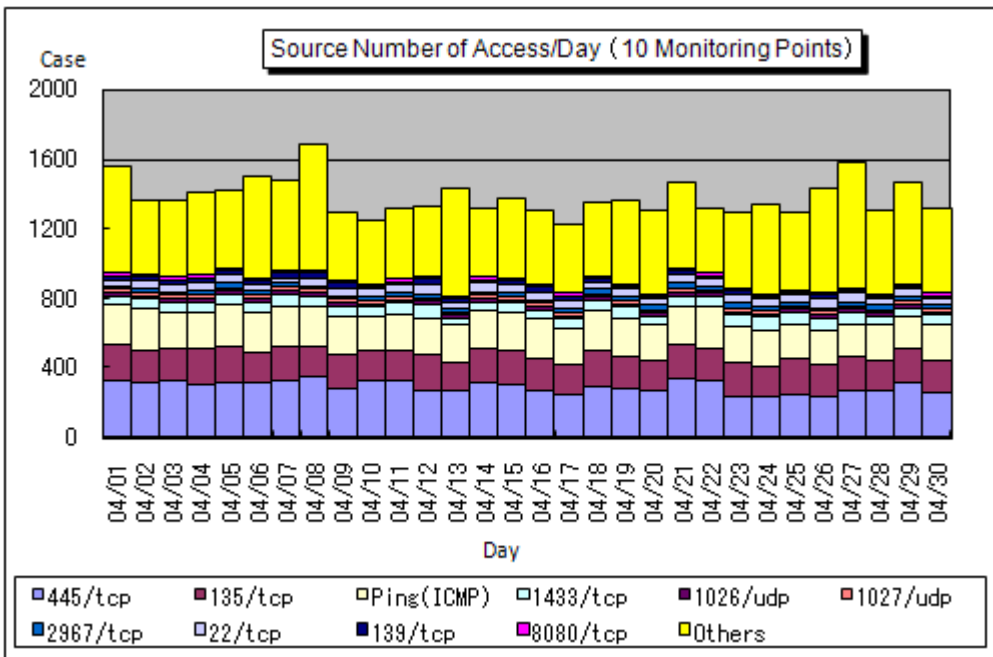
**2. Status for Unwanted (One-sided) Number of Access in April**

**(1) Accessing Status Classified by Destination (Port Type)**

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



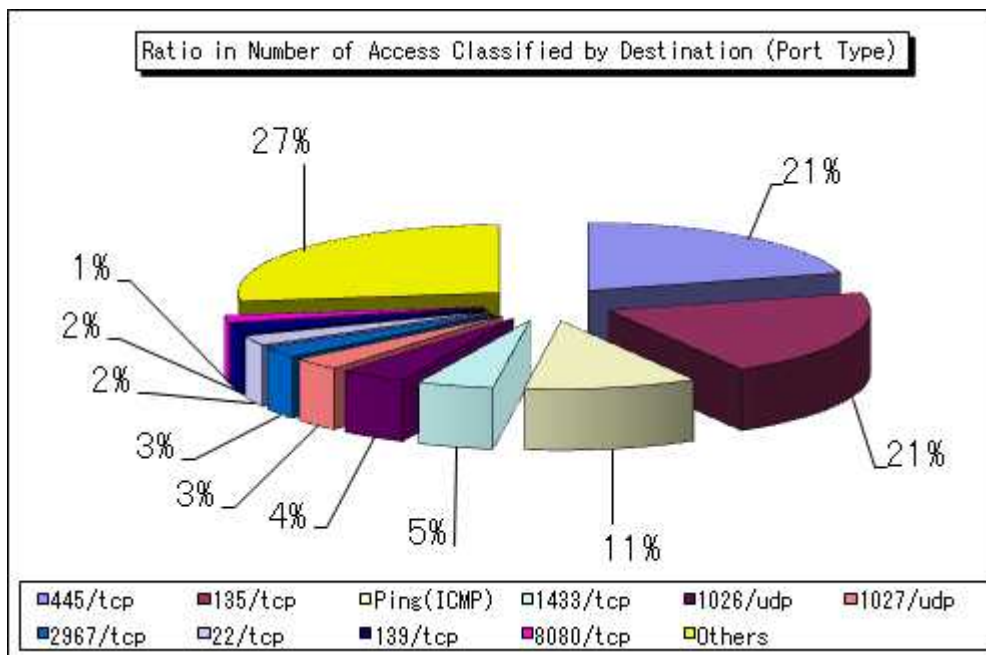
**Chart 2-1: Number of Access/Day in April 2009**



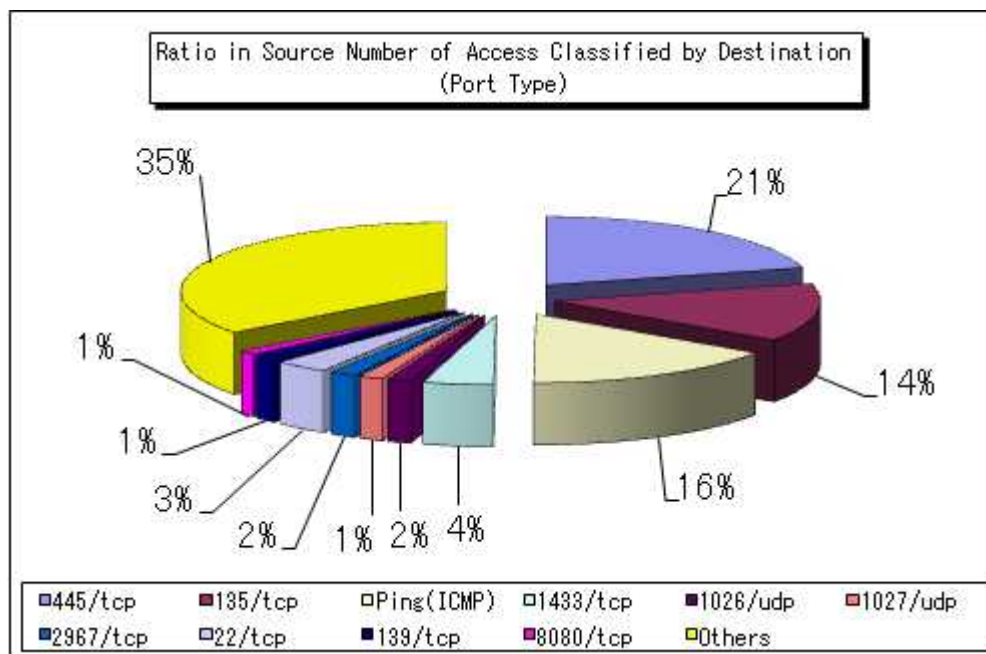
**Chart 2-2: Source Number of Access/Day in April 2009**

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

The Chart 2-3 shows the ratio in number of access classified by destination (port type) and the Chart 2-4 shows the ratio in source number of access classified by destination (port type) in April. For your information, numbers in ratio were rounded at the 1<sup>st</sup> arithmetic point so that the total may not make 100% sharp, accordingly.



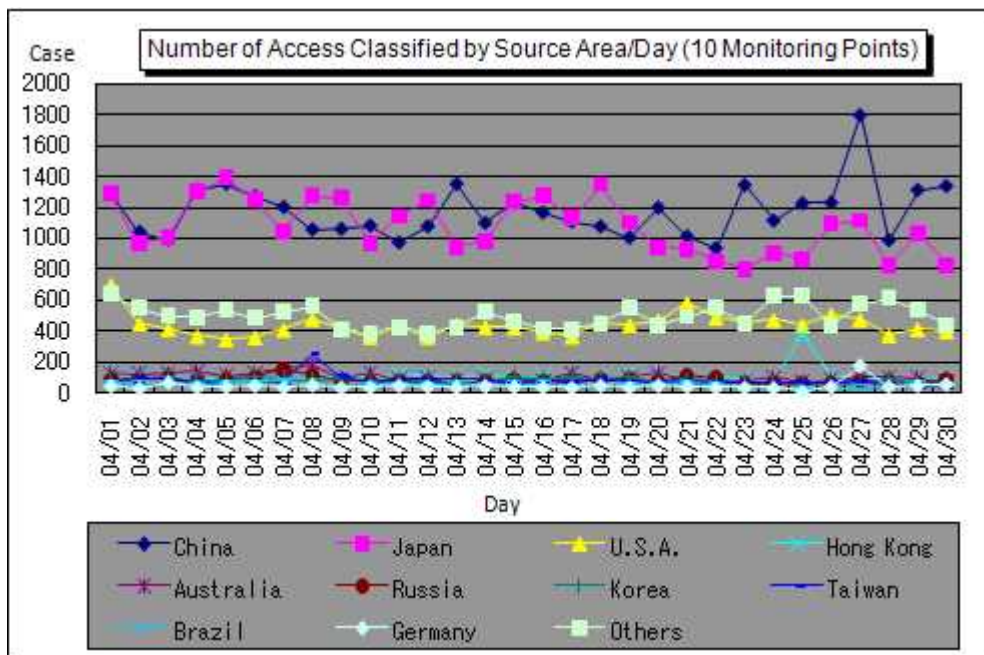
**Chart 2-3: Ratio in Number of Access Classified by Destination (Port Type) in April 2009**



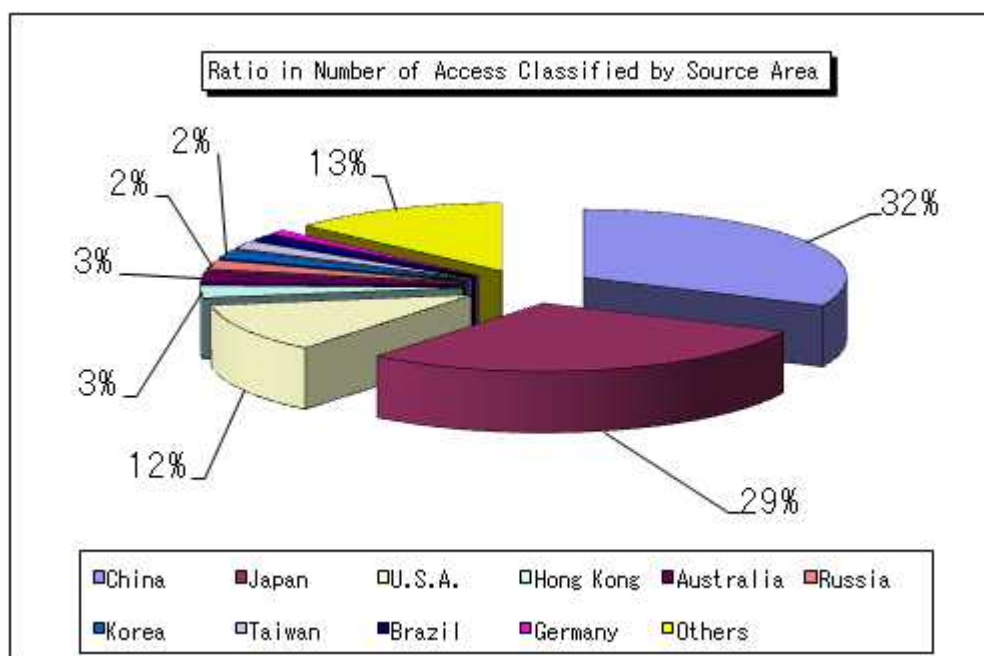
**Chart 2-4: Ratio in Source Number of Access Classified by Destination (Port Type) in April 2009**

**(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 April. For your information, numbers in ratio were rounded at the 1<sup>st</sup> arithmetic point so that the total may not make 100% sharp, accordingly.



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



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

The Chart 2-7 shows the 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 April. For your information, numbers in ratio were rounded at the 1<sup>st</sup> arithmetic point so that the total may not make 100% sharp, accordingly.

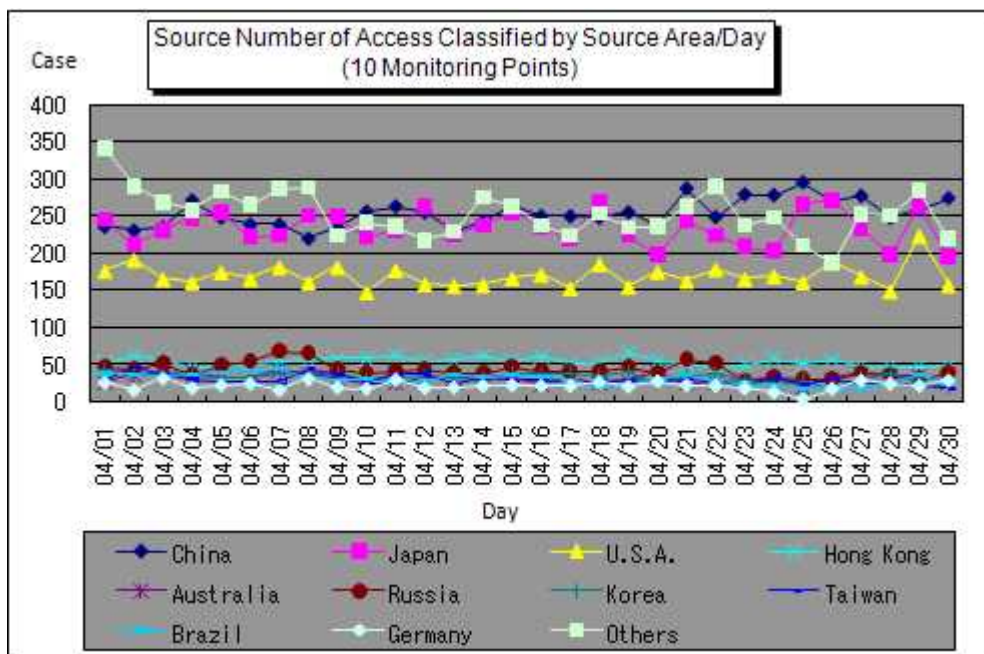


Chart 2-7: Source Number of Access Classified by Source Area/Day in April

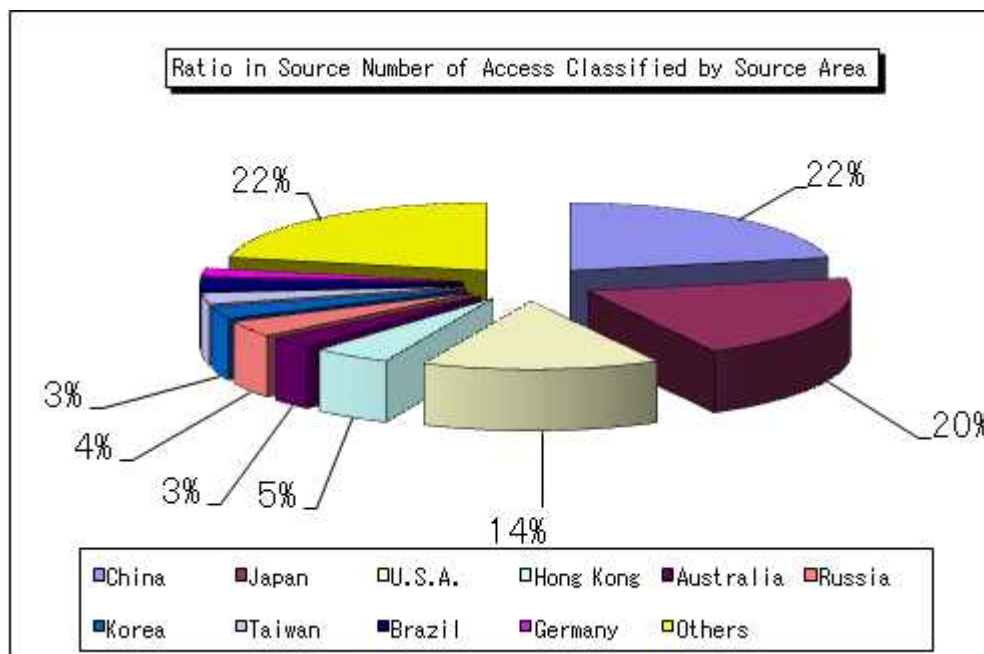
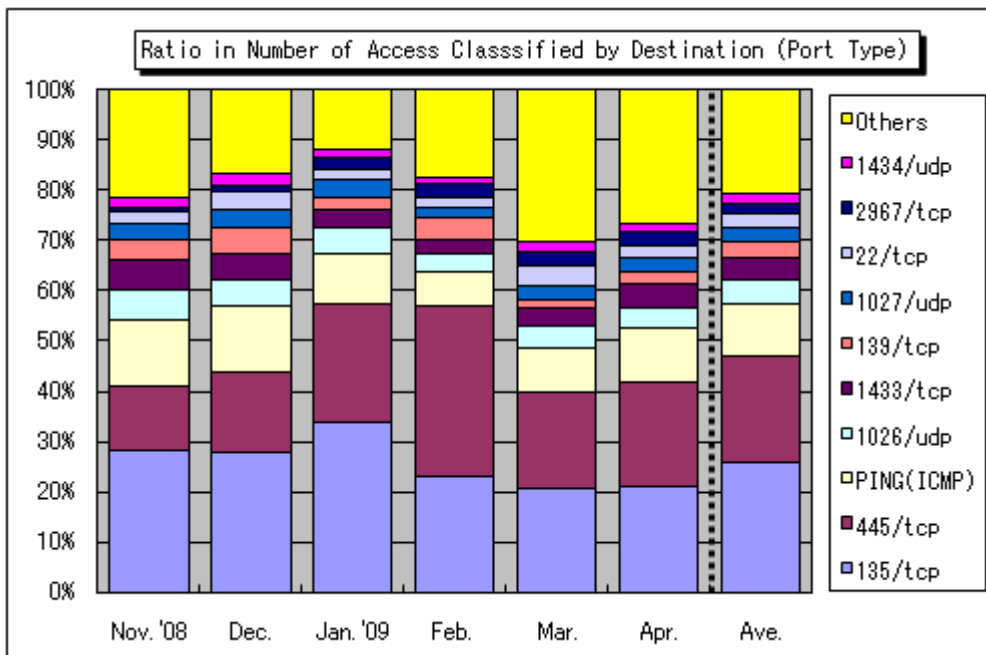


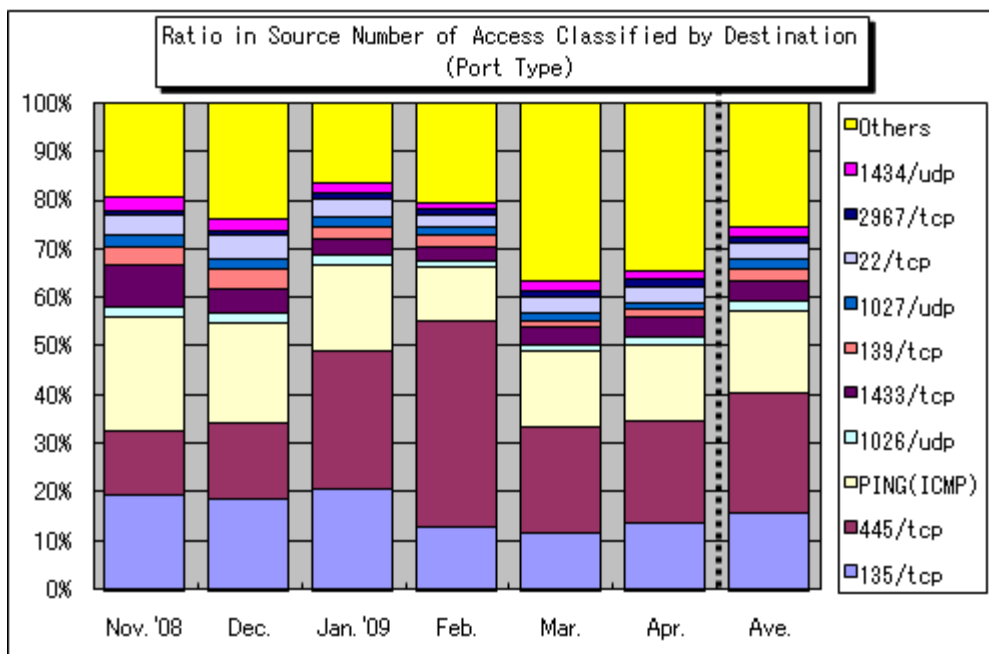
Chart 2-8: Ratio in Source Number of Access Classified by Source Area in April

**3. Statistical Information**

The Chart 3-1 shows the ratio in number of access classified by destination (port type) and the Chart 3-2 shows the ratio in source number of access classified by destination (port type) from November 2008 to April 2009.



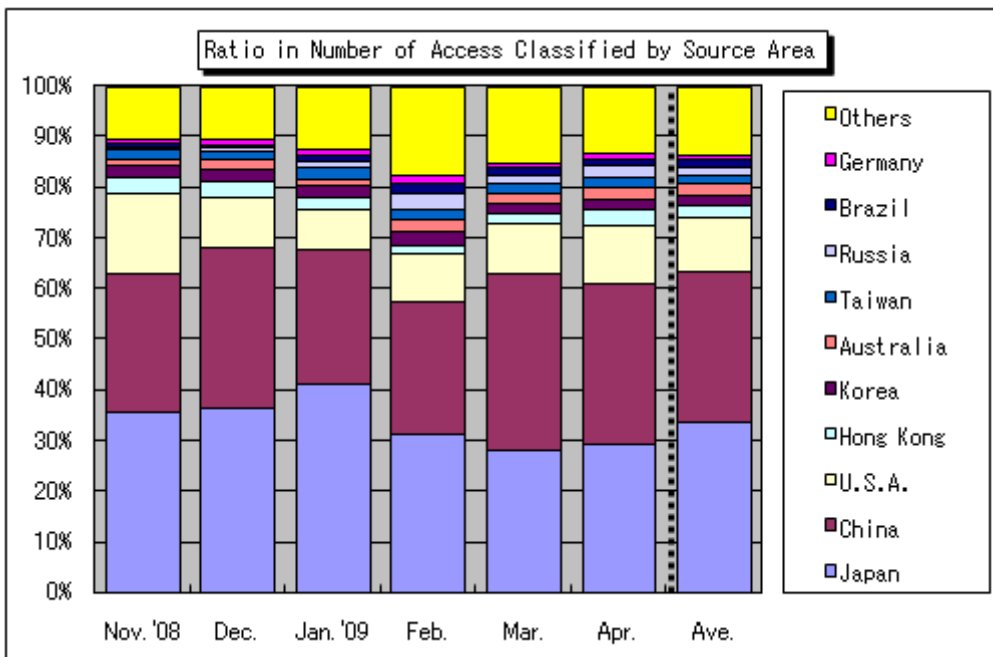
**Chart 3-1: Ratio in Number of Access Classified by Destination (Port Type) from November 2008 to April 2009**



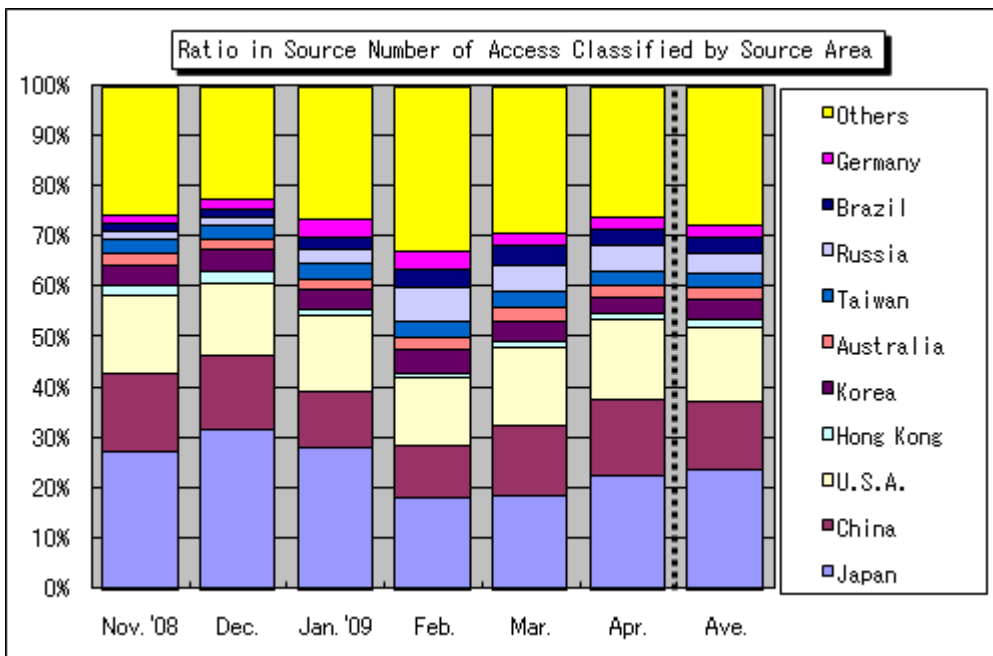
**Chart 3-2: Source Number of Access Classified by Destination (Port Type) from November 2008 to April 2009**

**(2) Ratio Classified by Destination**

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 November 2008 to April 2009.



**Chart 3-3: Ratio in Number of Access Classified by Source Area from November 2008 to April 2009**



**Chart 3-4: Ratio in Source Number of Access Classified by Source Area from November 2008 to April 2009**

#### 4. Supplementary Descriptions

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

Port Type	Interpretations/Descriptions
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.
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.
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.
139/tcp	Renowned to target those file sharing (network sharing) that has not been well-protected; generally, it is probable to be the accesses targeting vulnerabilities in Windows.
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.
1026/udp, 1027/udp	Renowned for sending pop-up (spam) messages exploiting Microsoft Windows Messenger service which differs from MSN Messenger.
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.
2967/tcp	High potential of access which targets vulnerability in Symantec products.
8080/tcp	This is the most commonly accessed port to connect to HTTP proxy so that the access is very much exploitable to search proxy server that can be used as a steppingstone server by a malicious intent.

***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)