

## Report from the Internet Monitoring (TALOT2)

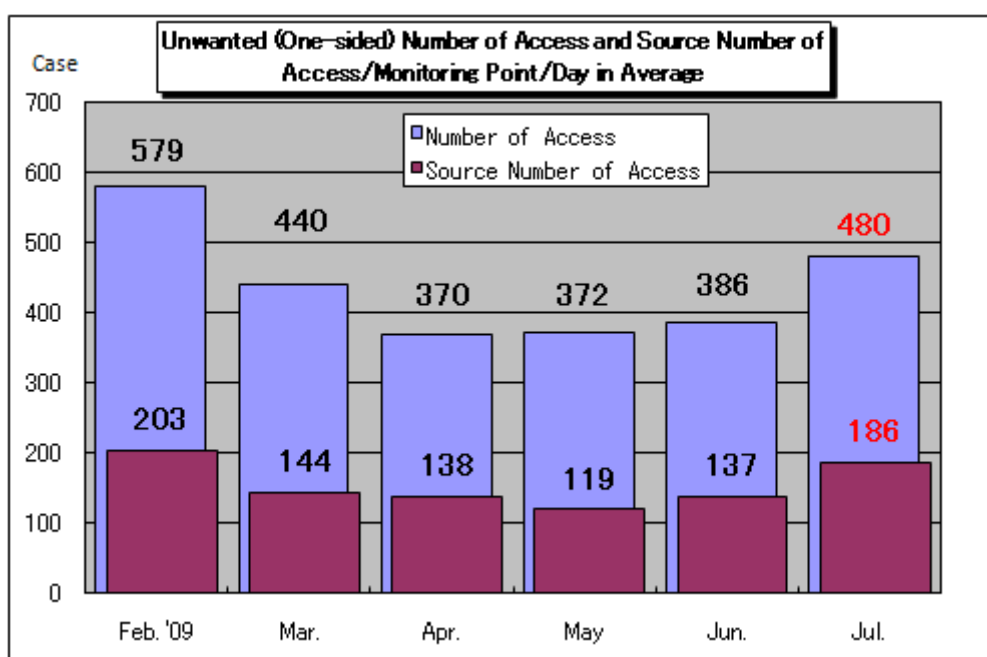
July 2009

### 1. To the General Internet Users

In the Internet Monitoring (TALOT2), unwanted (one-sided) access in June totaled **148,935** cases for the 10 monitoring points and the gross number of the sources\* was **57,687**: unwanted (one-sided) access captured at one monitoring point was **480** accesses from **186** 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 in Average**

The Chart 5-1 shows the unwanted (one-sided) number of access and the source number of access/monitoring point/day from February to July 2009. Both unwanted (one-sided) number of accesses were increased compared with those in June.

The Chart 5-2 shows the comparison of number of access classified by destination (by port) for June and July. In July, the access to the port 445/tcp was further increased from the one in June. The cause of access increase in June was that the number of access from overseas was increased: this scenario was still continued in July: thereby the access increased to the port 445/tcp (See the Chart 5-3). The cause for that access increase has not yet been clarified: as with June, the number of access from overseas further increased, but none of number of access from specific source was increased.

In July, access to several ports such as 22862/tcp, 12370/udp, 7259/udp, etc. were monitored: they were the ports that none of access was monitored in June. The cause for their accesses to these ports was unknown; they were monitored at single specific monitoring point respectively.

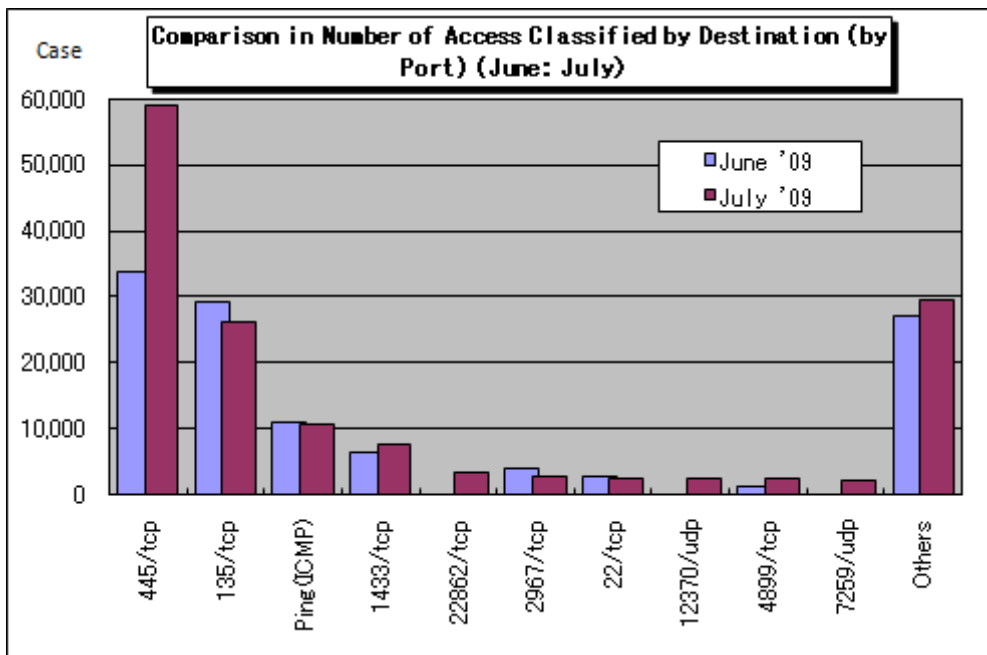


Chart 1-2: Comparison in Number of Access Classified by Destination (by Port) (June: July)

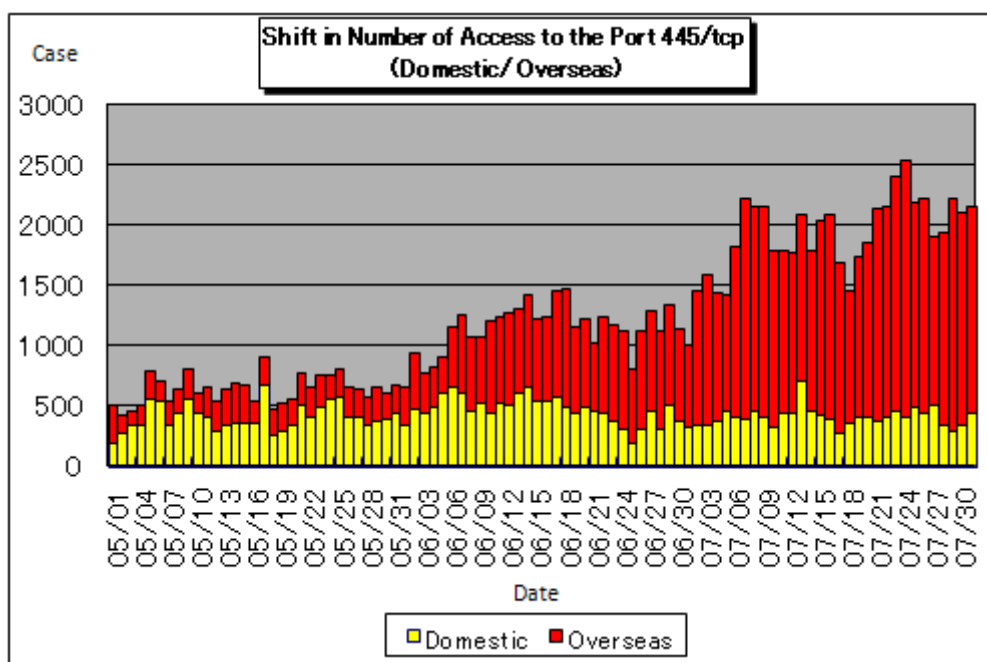
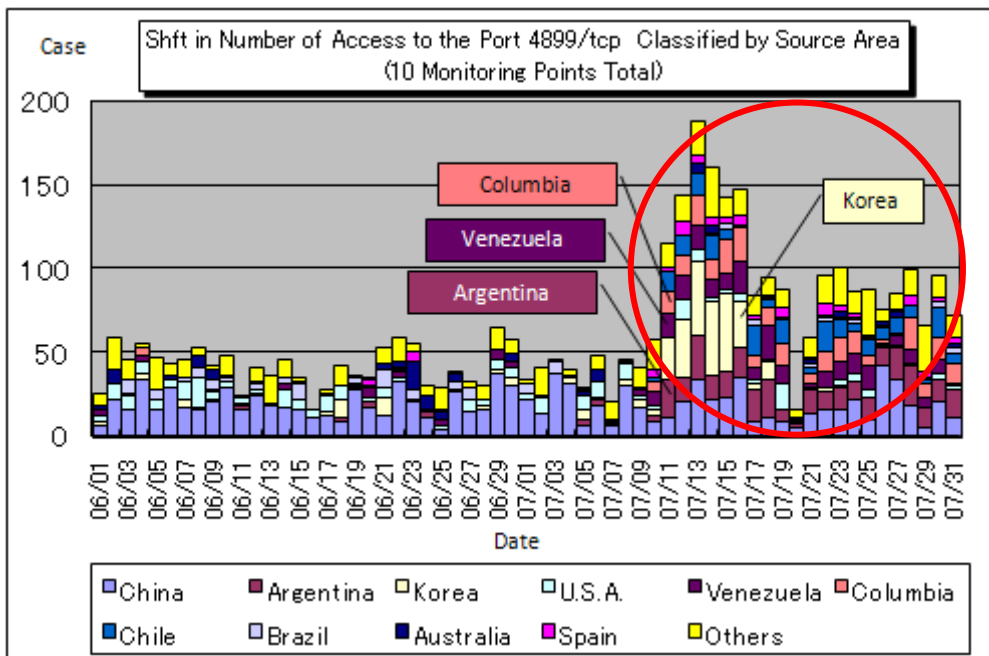


Chart 1-3: Shift in Number of Access to the Port 445/tcp (Domestic/Overseas)

**2. Access to the Port 445/tcp**

In the middle of July, there is a period for which access to the port 4899/tcp was increased, but temporarily. This was the cause that the access from one of Korean sources and accesses from several sources from South America such as Argentina, Venezuela, Columbia, etc. were increased (See the Chart 2-1).



**Chart 2-1: Shift in Number of Access to the Port 4899/tcp Classified by Destination (10 Monitoring Points Total)**

The access increase to the port 4899/tcp from South America was also monitored by the other organizations where conduct fixed-point observation: in another words, similar event may have been caused over a quite wide area.

The port 4899/tcp was known as the port used by Radmin, the remote control software by Famatech.

Accordingly, those Radmin users should check if your computer is not allowing access to the port 4899/tcp from unauthorized source (s). Be sure to restrict access to the port (squeezing of IP address to be allowed for access) and/or to harden access authentication.

### 3. Unwanted (One-sided) Accessing Status in July 2009

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

The Chart 3-1 shows the shift in unwanted (one-sided) accessing status (number of access) and the Chart 3-2 shows the shift in unwanted (one-sided) accessing status (source number of access) in July 2009.

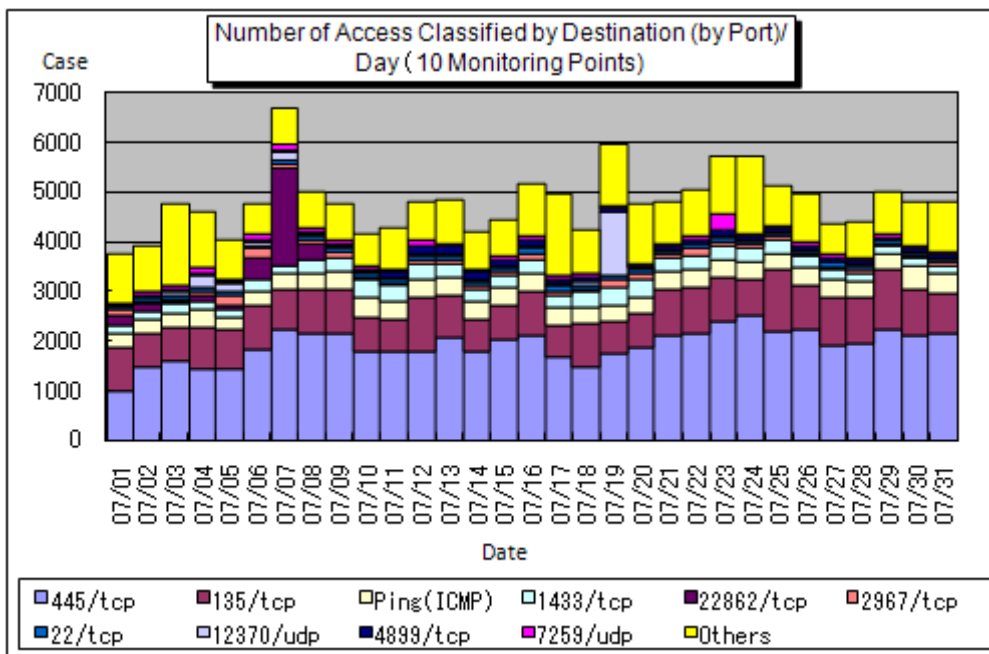


Chart 3-1: Number of Access Classified by Destination (by Port) /Day in July 2009

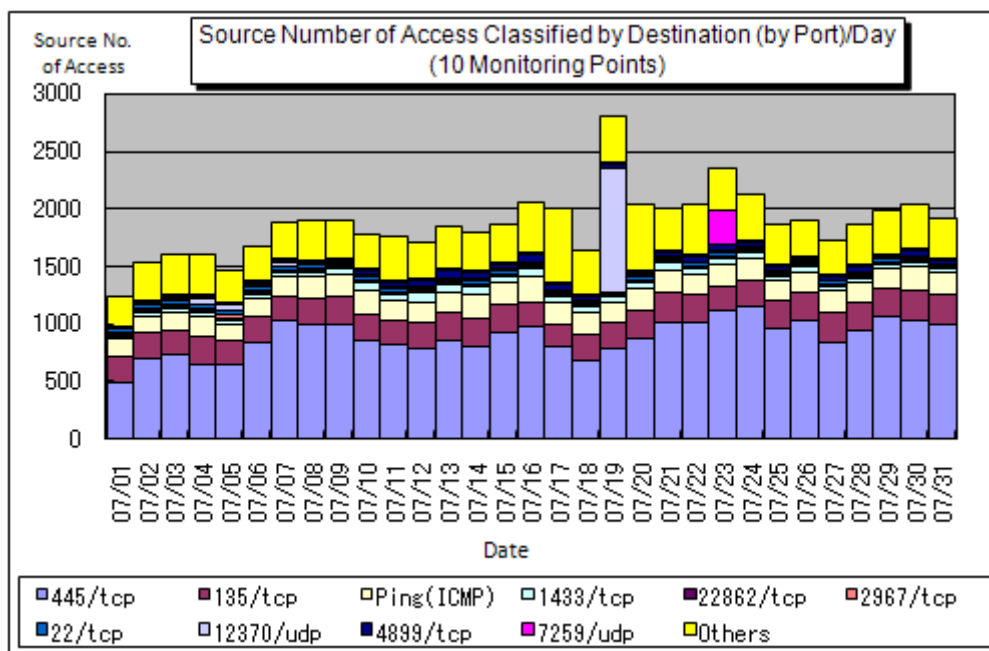


Chart 3-2: Source Number of Access Classified by Destination (by Port) /Day in July 2009

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

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

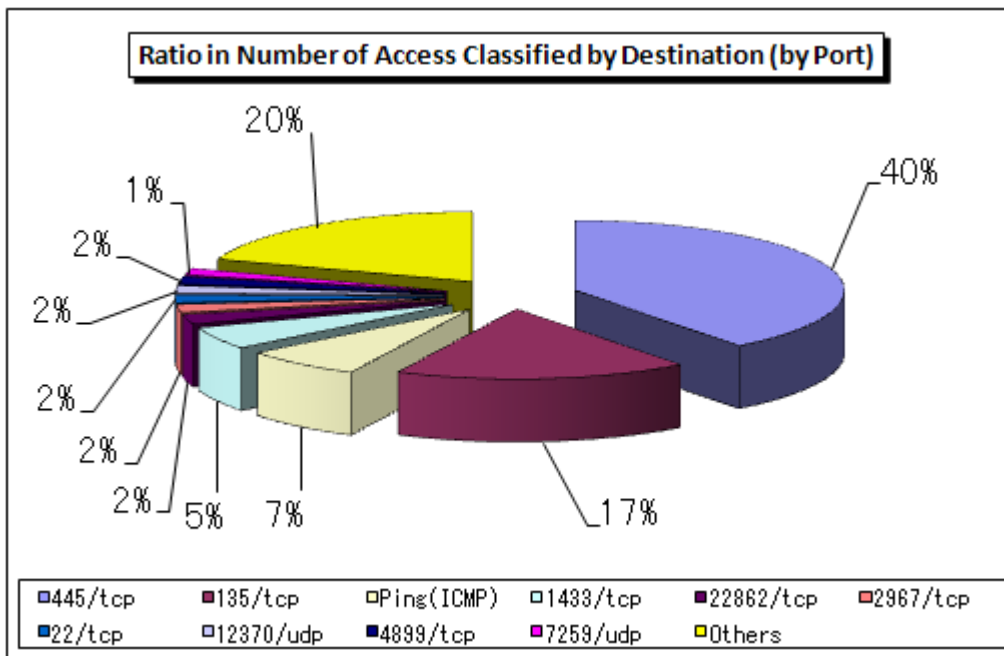


Chart 3-3: Ratio in Number of Access Classified by Destination (by Port) in July 2009

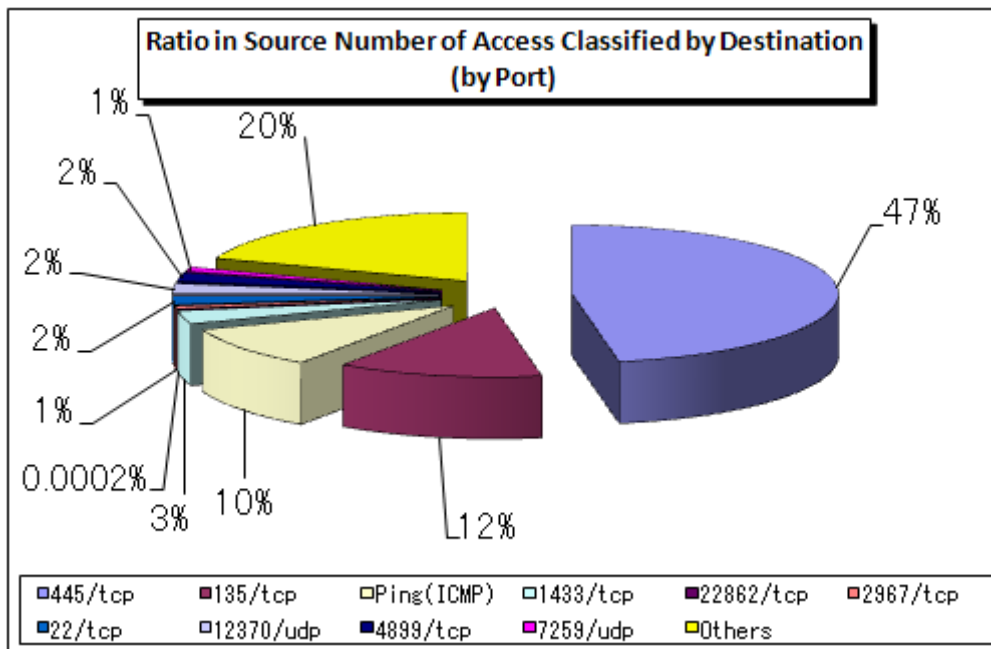


Chart 3-4: Ratio in Source Number of Access Classified by Destination (by Port) in July 2009

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

The Chart 3-5 shows the shift in number of access classified by unwanted (one-sided) source area and the Chart 3-6 shows the ratio in number of access classified by source area. For your further information, numbers in ratio are rounded at the 1<sup>st</sup> decimal point so that they may not make 100% sharp, accordingly.

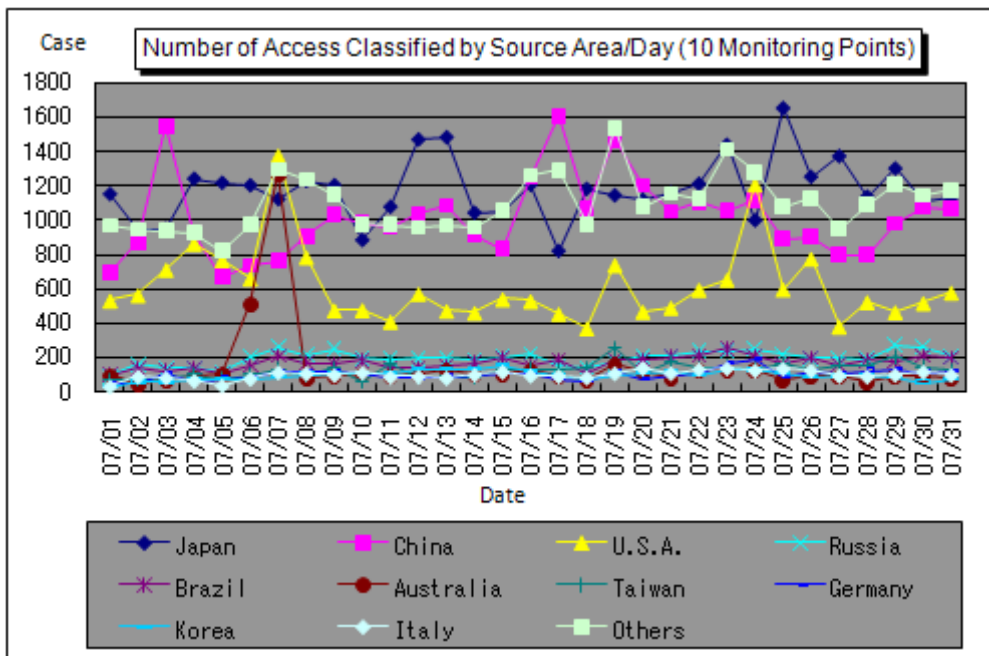


Chart 3-5: Number of Access Classified by Source Area/Day in July 2009

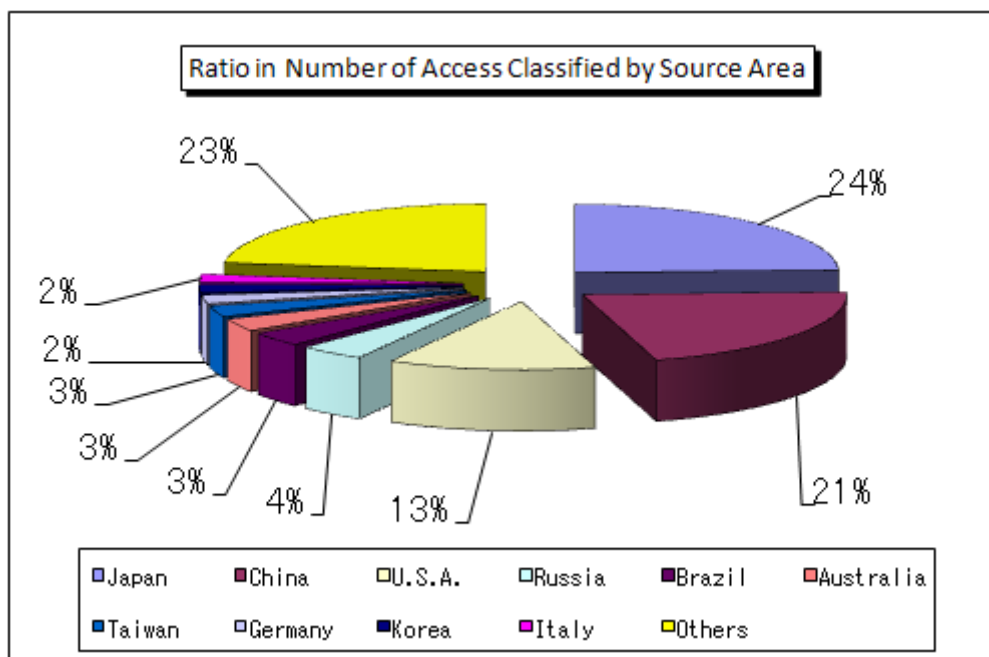


Chart 3-6: Ratio in Number of Access Classified by Source Area in July 2009

The Chart 3-7 shows the shift in source number of access classified by source area and the Chart 3-8 shows the ratio in source number of access classified by source area in July 2009. For your further information, numbers in ratio are rounded at the 1<sup>st</sup> decimal point so that they may not make 100% sharp, accordingly.

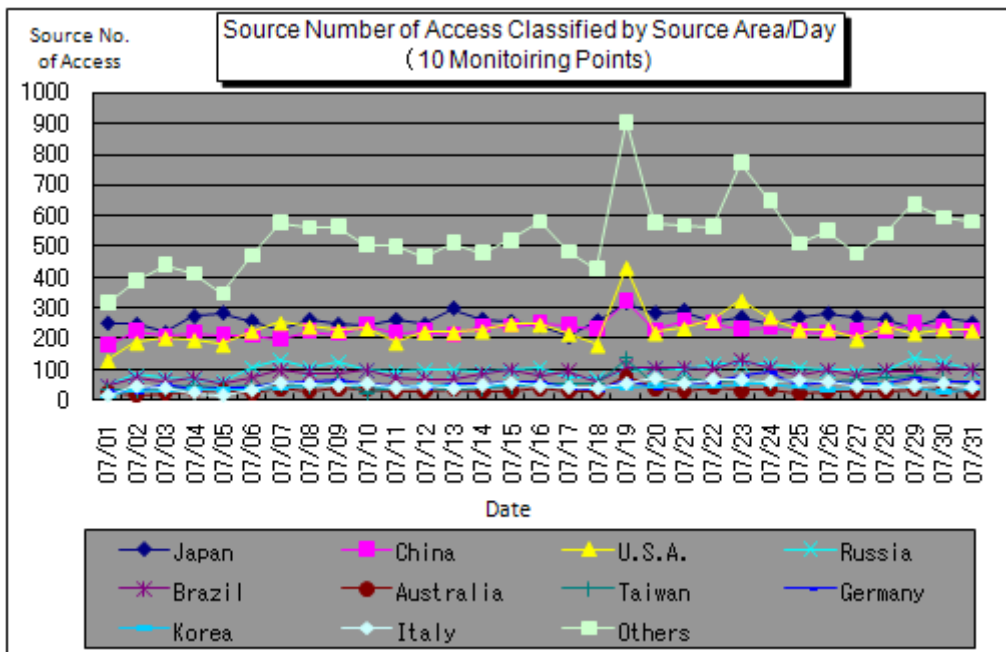


Chart 3-7: Shift in Source Number of Access Classified by Source Area/Day in July 2009

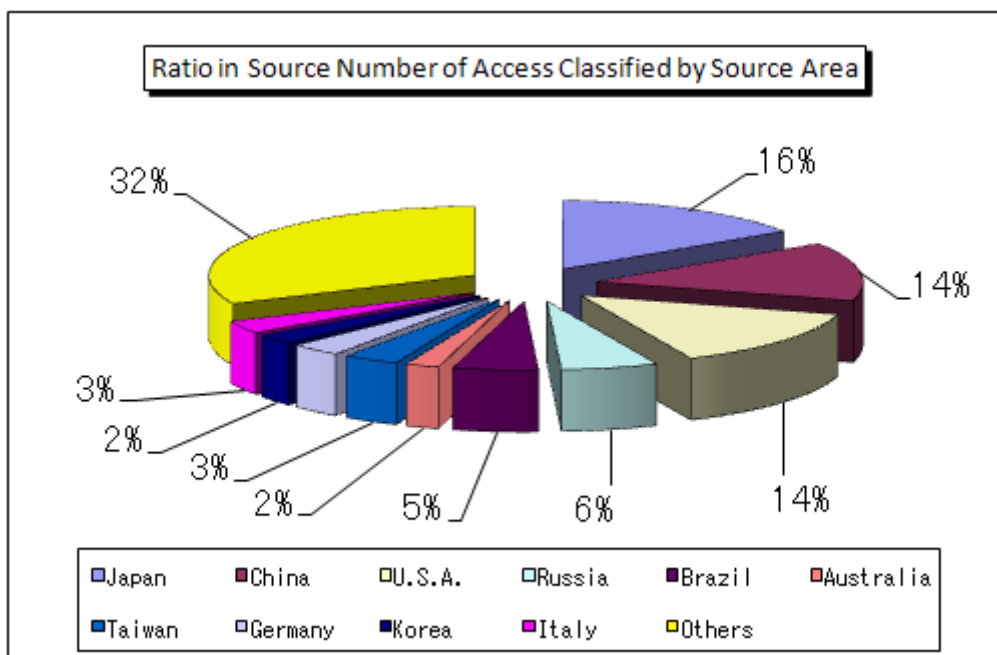


Chart 3-8: Ratio in Source Number of Access Classified by Source Area in July 2009

4. Statistical Information

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

Chart 4-1 shows the ratio in number of access classified by destination (by port) and the Chart 4-2 shows the ratio in source number of access classified by destination (by port) from February to July 2009.

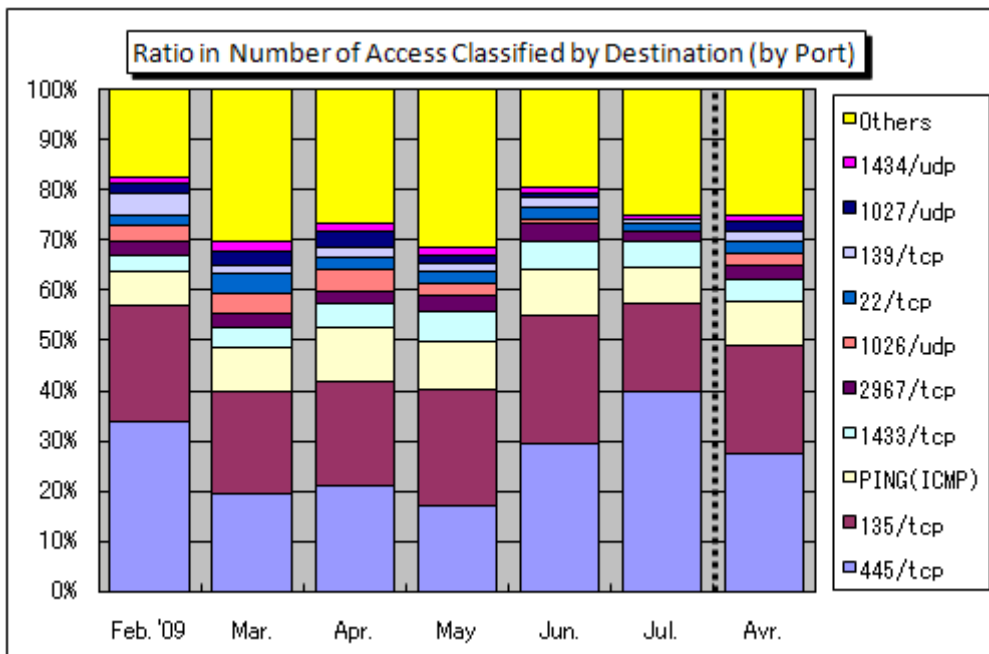


Chart 4-1: Ratio in Number of Access Classified by Destination (by Port) from February to July 2009

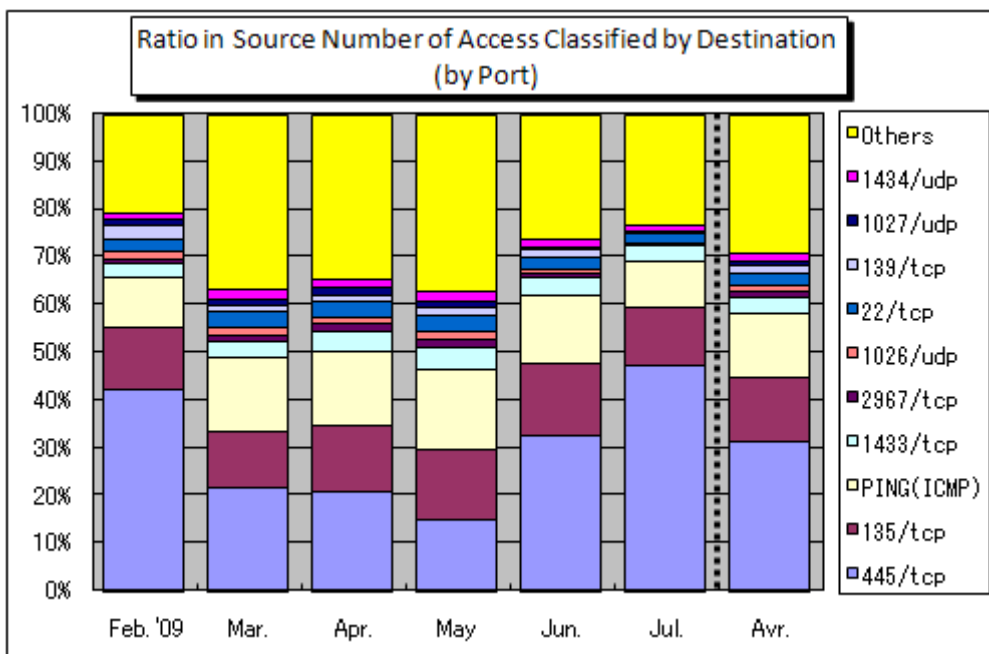


Chart 4-2: Ratio in Source Number of Access Classified by Destination (by Port) from February to July 2009

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

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

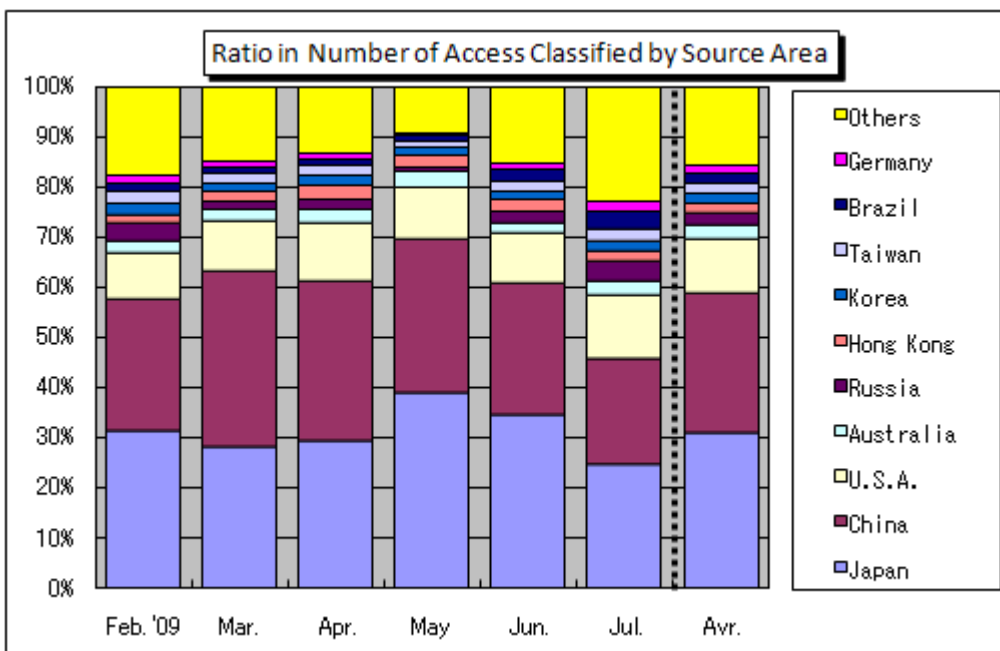


Chart 4-3: Ratio in Number of Access Classified by Source Area from February to July 2009

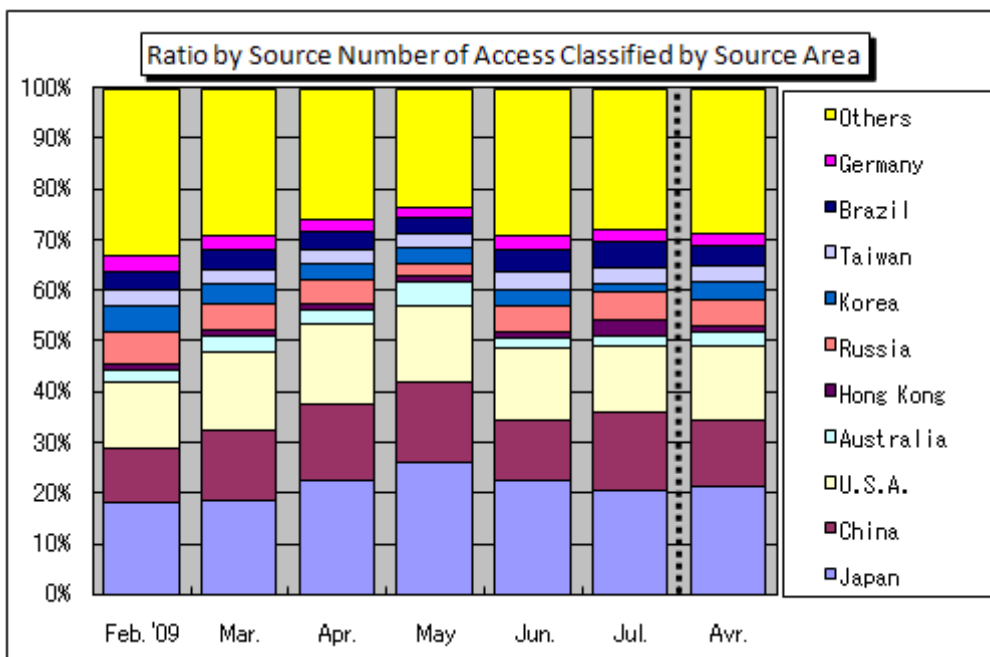


Chart 4-4: Ratio in Source Number of Access Classified by Source Area from February to July 2009

## 5. Supplementary Descriptions

Following are the explanations for the destination (port type) remarkably accessed (either in-bound or out-bound or both) in July 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.
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.
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 such as Symantec Client Security and Symantec AntiVirus, 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).
7259/tcp	The access monitored by single monitoring point from multiple source number of accesses: the cause is unknown.
12370/udp	The access monitored by single monitoring point from multiple source number of accesses: the cause is unknown.
22862/tcp	The access monitored by single monitoring point from minor and specific source number of access: the cause is unknown.

### **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)