

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

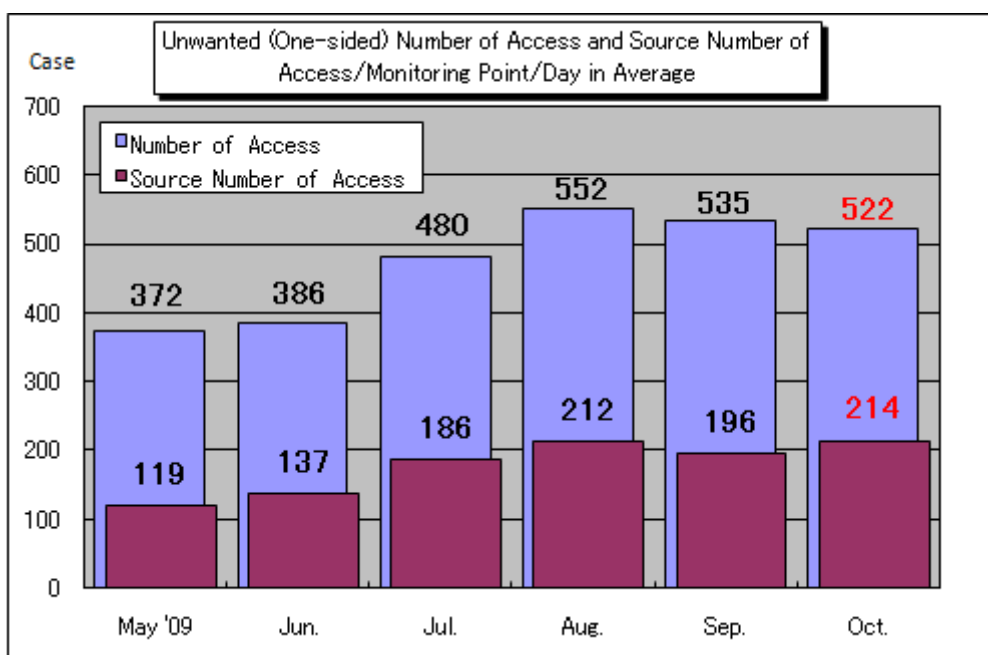
October 2009

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

In the Internet Monitoring (TALOT2), unwanted (one-sided) access in October totaled **161,716** cases for the 10 monitoring points and the gross number of the sources\* was **66,430**: unwanted (one-sided) access captured at one monitoring point was **522** accesses from **214** 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 and the source number of access/monitoring point/day from May to October 2009. Both the unwanted (one-sided) number of accesses in October were subtly decreased from the ones in September.

The Chart 5-2 shows the comparison in number of access classified by destination (by port) in September and October. As the graph shows, the access to the port 445/tcp was increased about 40% from the one in September.

The port 445/tcp is one of the renowned ports to be targeted by the viruses and worms which exploit vulnerability (MS08-067) in Windows. The vulnerability (MS09-050) in SMB(\*v2 in Windows publicized by Microsoft on October 13, 2009 (U.S.time) was also relevant to the port 445/tcp.

In TALOT2, such access increase to the port 445/tcp had been monitored on and around the vulnerability information was publicized, there may have been some malicious activities which attempted to exploit this vulnerability (see the Chart 5-3). Since this vulnerability can be permanently addressed by applying the modification program which provided by Microsoft on the day the vulnerability was publicized: accordingly, be sure to apply it immediately for your further security.

(\*) SMB is referred as Server Message Block. This is the one of file sharing protocols to be used by the computer on Windows by default. SMBv2 (SMB Version 2.0) is the up-dated version for the default SMB and only supported by Windows Server 2008, Windows 7 and Windows Vista.

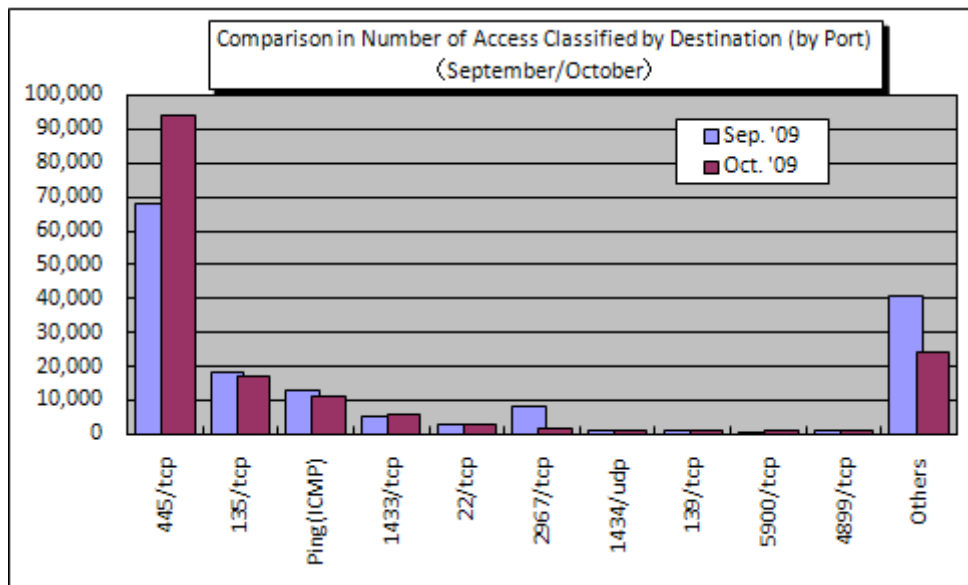


Chart 1-2: Comparison in Number of Access by Destination (by Port) (September: October)

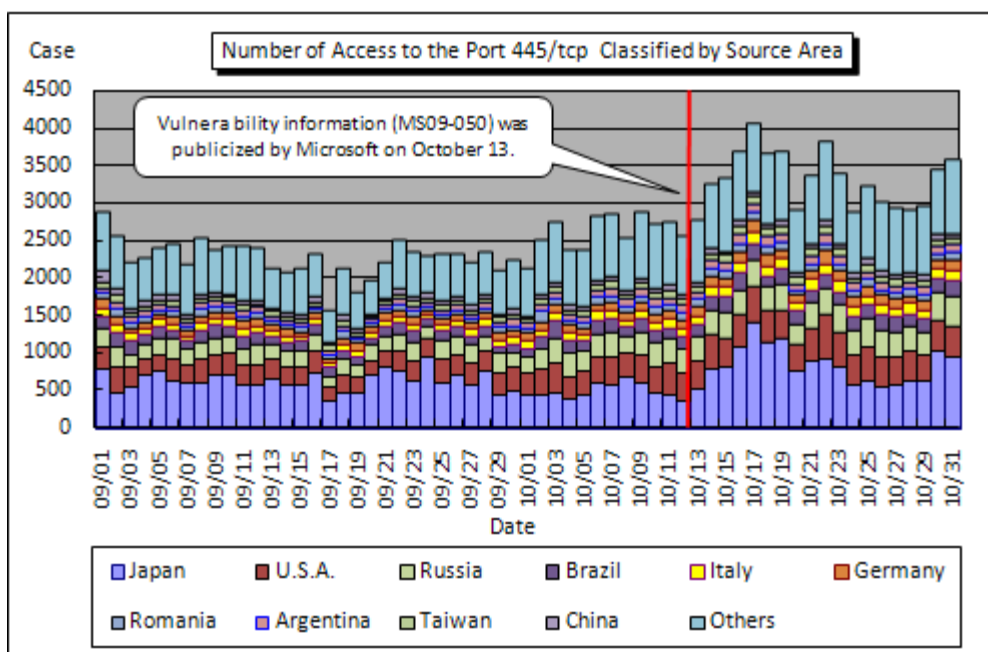


Chart 1-3: Number of Access to the Port 445/tcp Classified by Source Area (10 Monitoring Points Total)

<Reference>

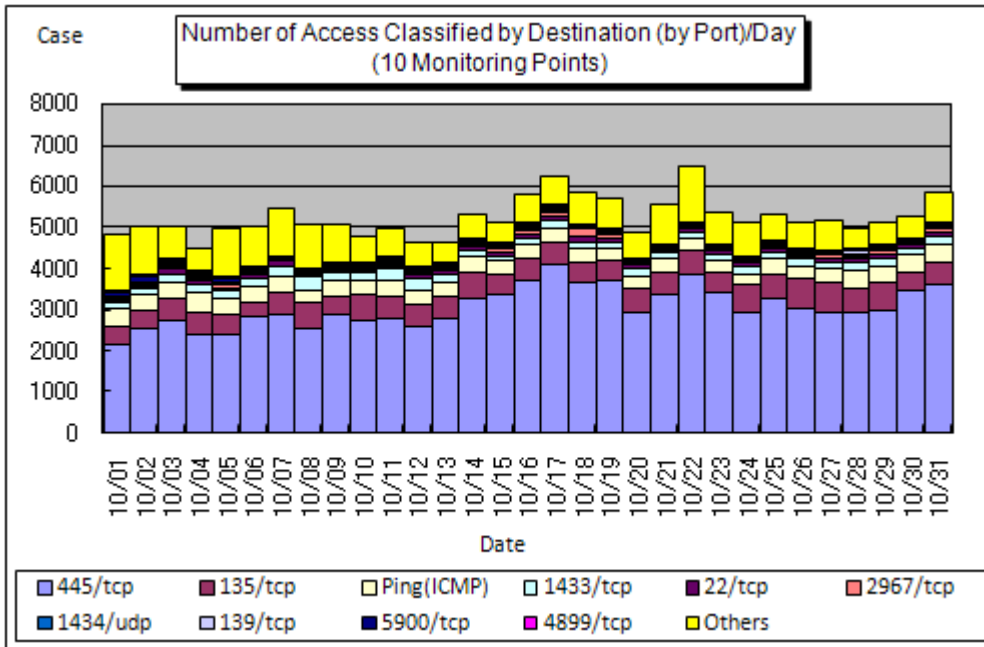
“Vulnerabilities in SMB could allow remote code execution” (Microsoft)  
<http://www.microsoft.com/technet/security/bulletin/MS09-050.msp>

“Information relevant to the vulnerability (MS09-050) in MSBv2 in Microsoft Windows” (IPA)  
<http://www.ipa.go.jp/security/ciadr/vul/20091014-ms09-050.html>

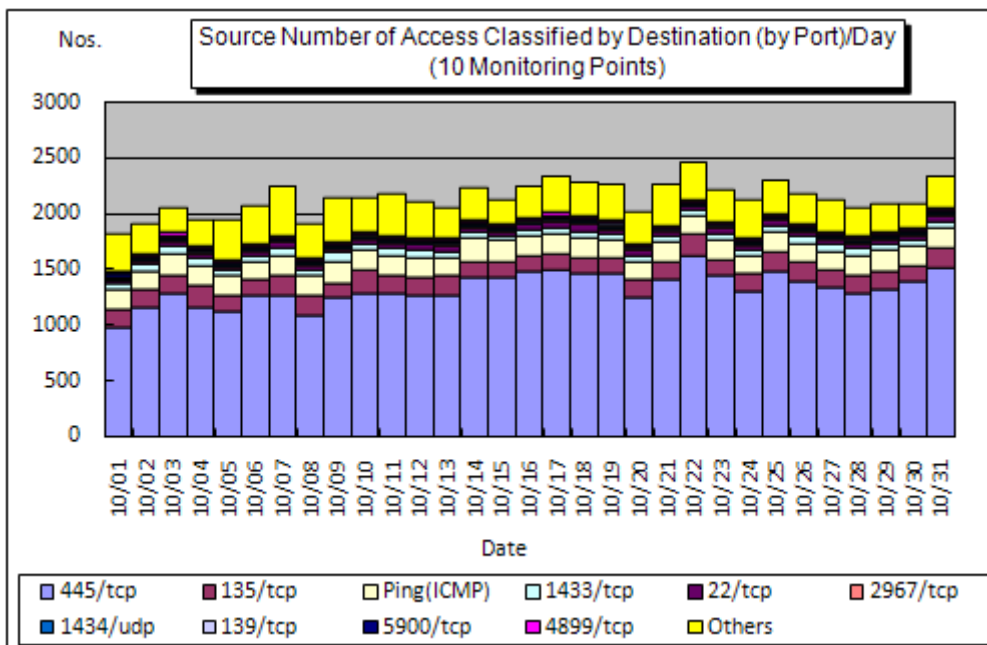
**2. Status for Unwanted (One-sided) Number of Access in October 2009**

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

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



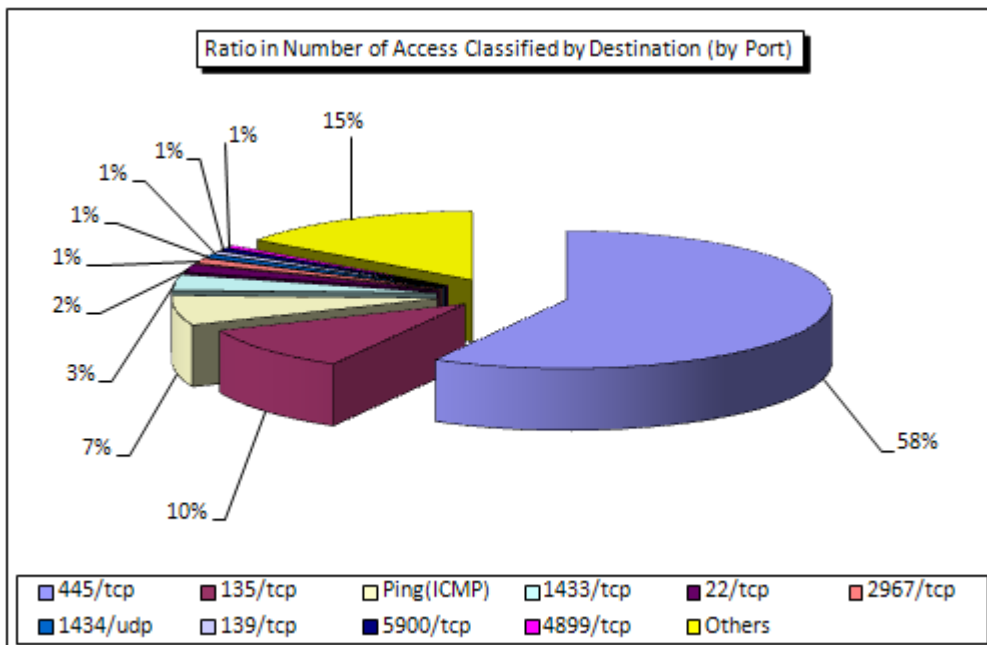
**Chart 2-1: Number of Access Classified by Destination (by Port)/Day in October 2009**



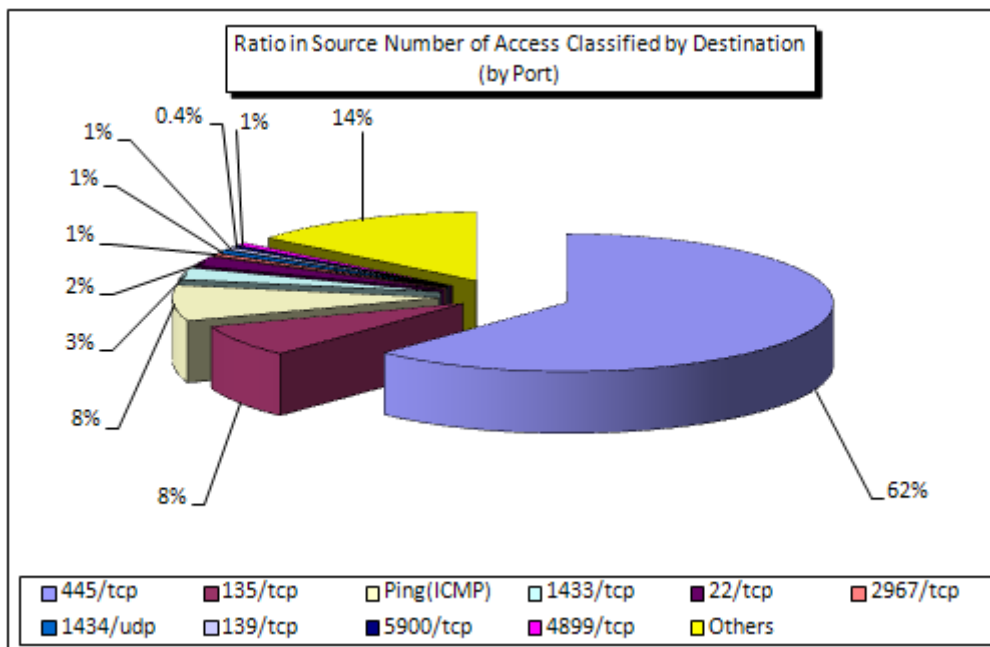
**Chart 2-2: Source Number of Access Classified by Destination (by Port)/Day in October 2009**

**(2) Ratio in 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 October 2009. For your further information, numbers in ratio were rounded at the 1<sup>st</sup> arithmetic point so that their total may not make 100% sharp, accordingly.



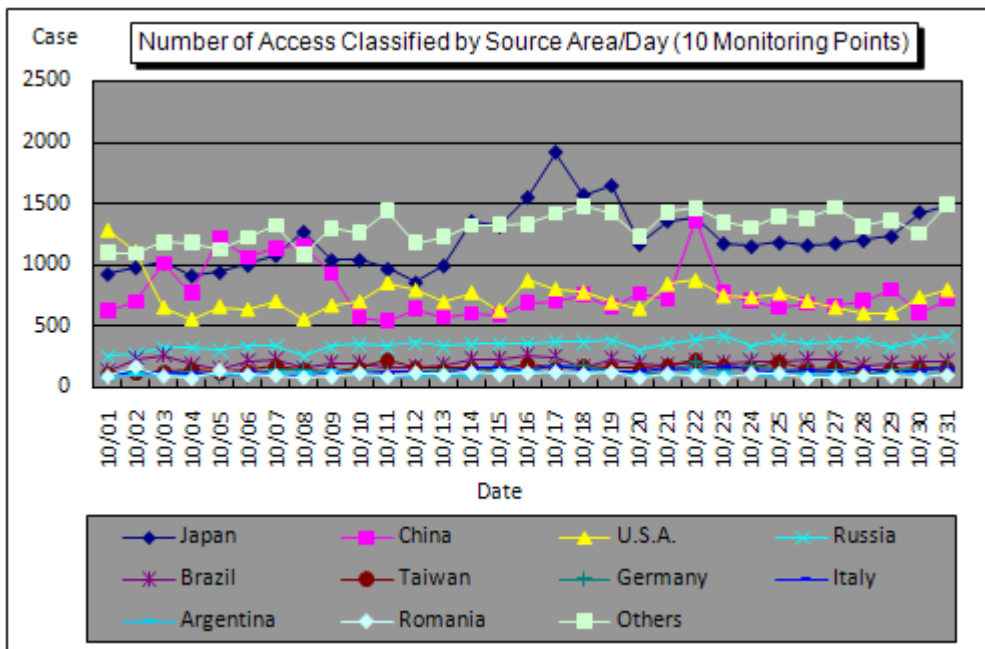
**Chart 2-3: Ratio in Number of Access Classified by Destination (by Port) in October 2009**



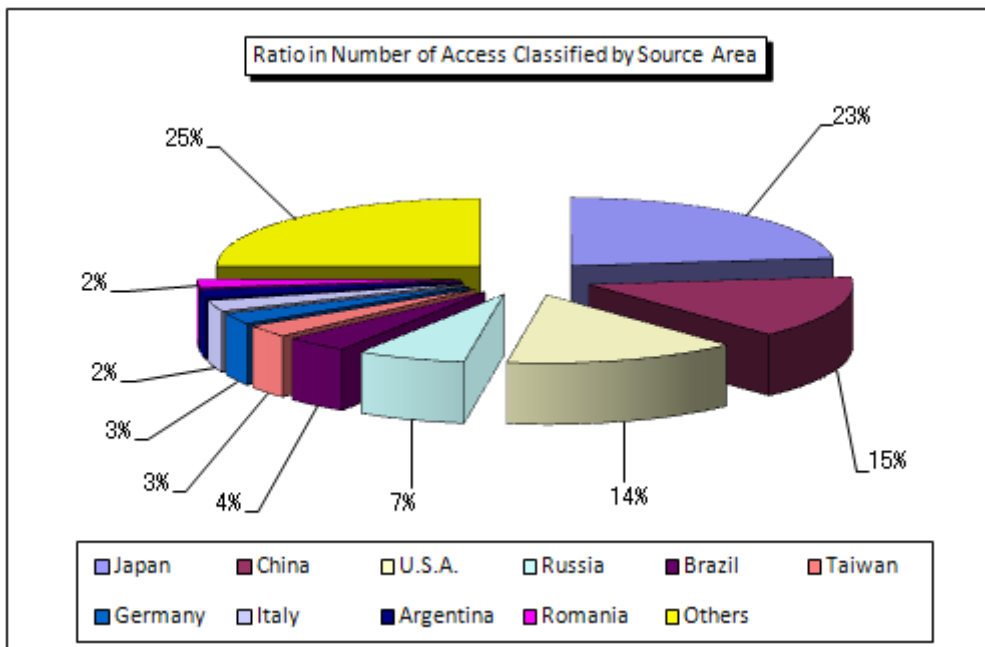
**Chart 2-4: Ratio in Source Number of Access Classified by Destination (by Port) in October 2009**

**(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 October 2009. For your further information, numbers in ratio were rounded at the 1<sup>st</sup> arithmetic point so that their total may not make 100% sharp, accordingly.

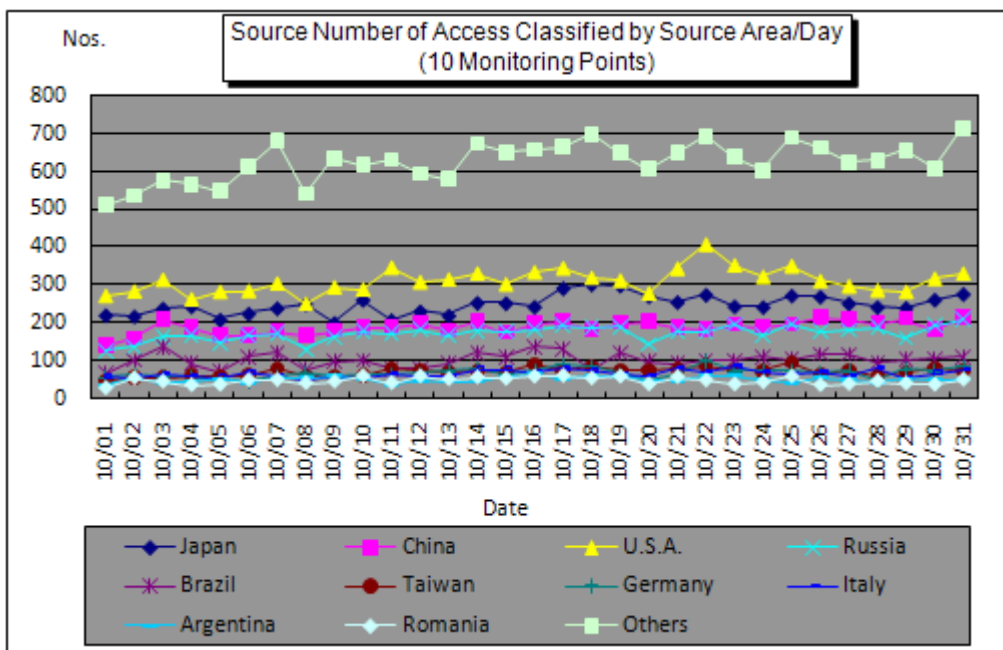


**Chart 2-5: Number of Access Classified by Source Area/Day in October 2009**

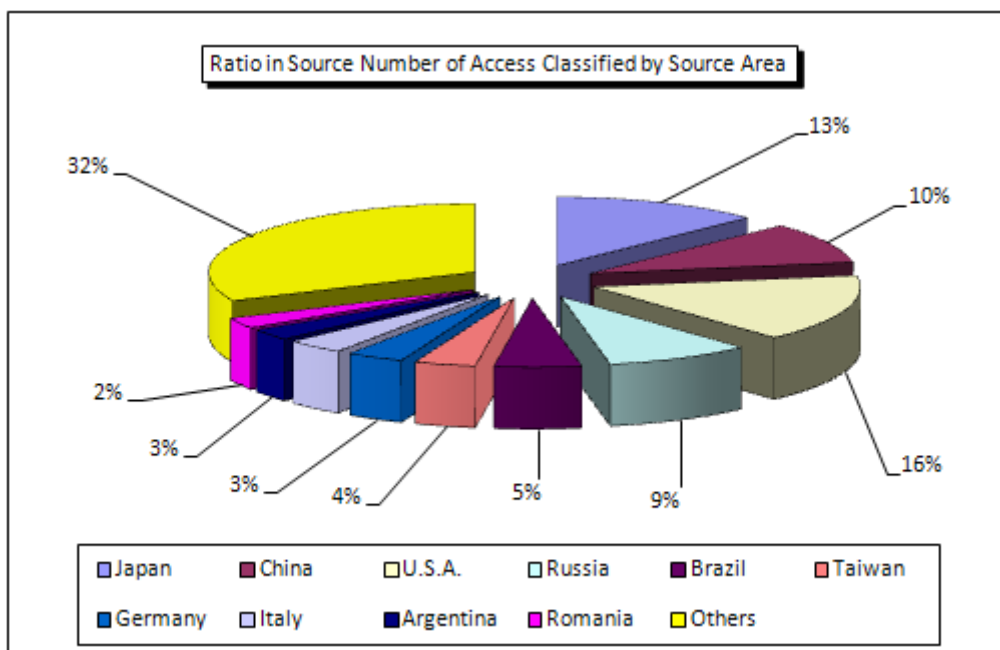


**Chart 2-6: Ratio in Number of Access Classified by Source Area in October 2009**

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 October 2009. For your further information, the numbers in ratio were rounded at the 1<sup>st</sup> arithmetic point so that their total may not make 100% sharp, accordingly.



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

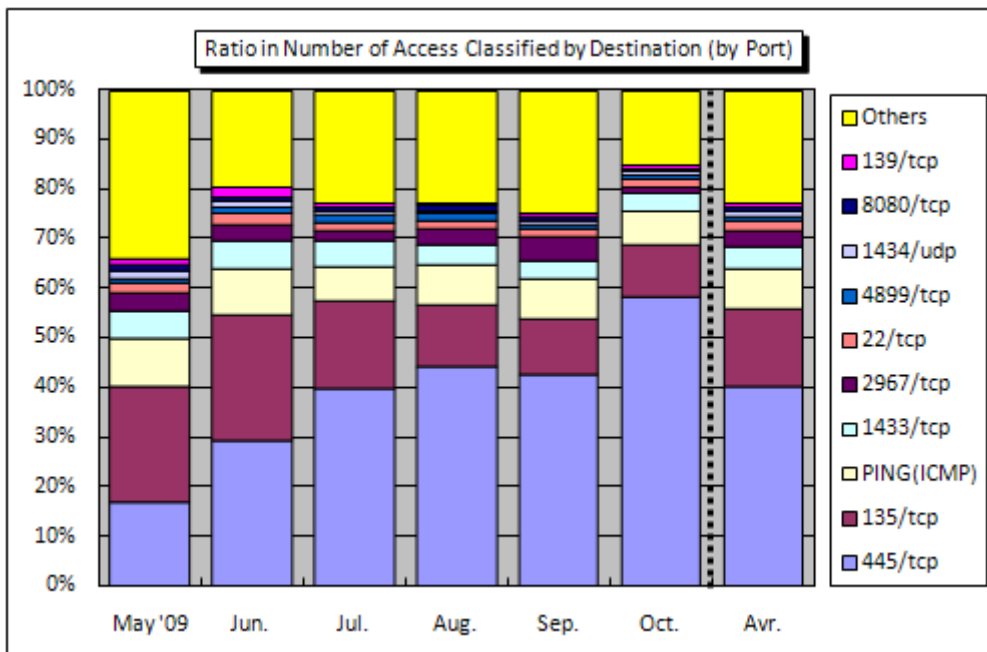


**Chart 2-8: Ratio in Source Number of Access Classified by Source Area in October 2009**

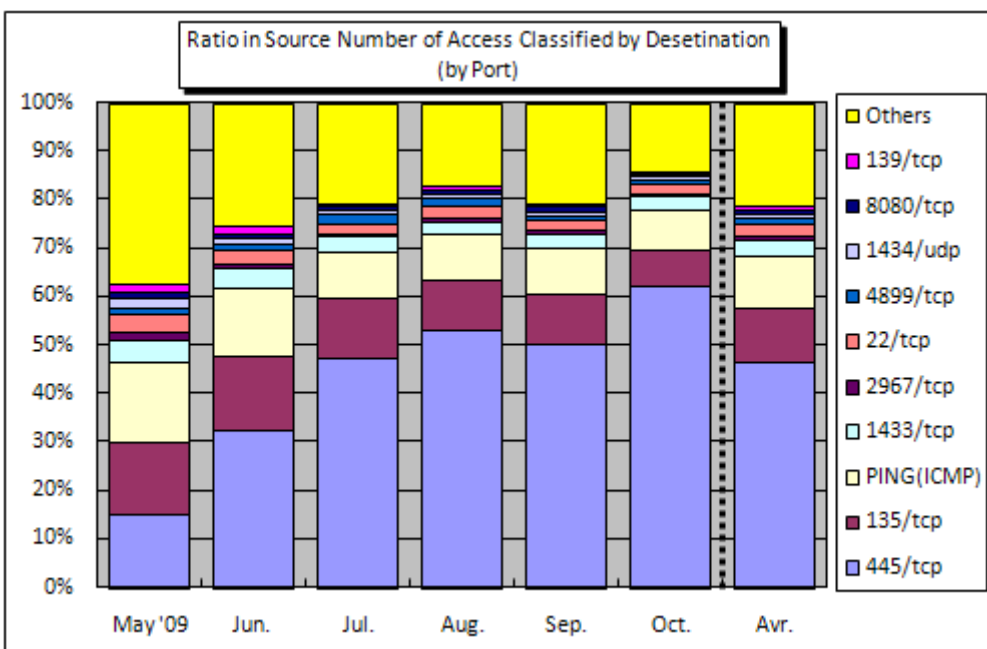
### 3. Statistical Information

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

The 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 May to October 2009.



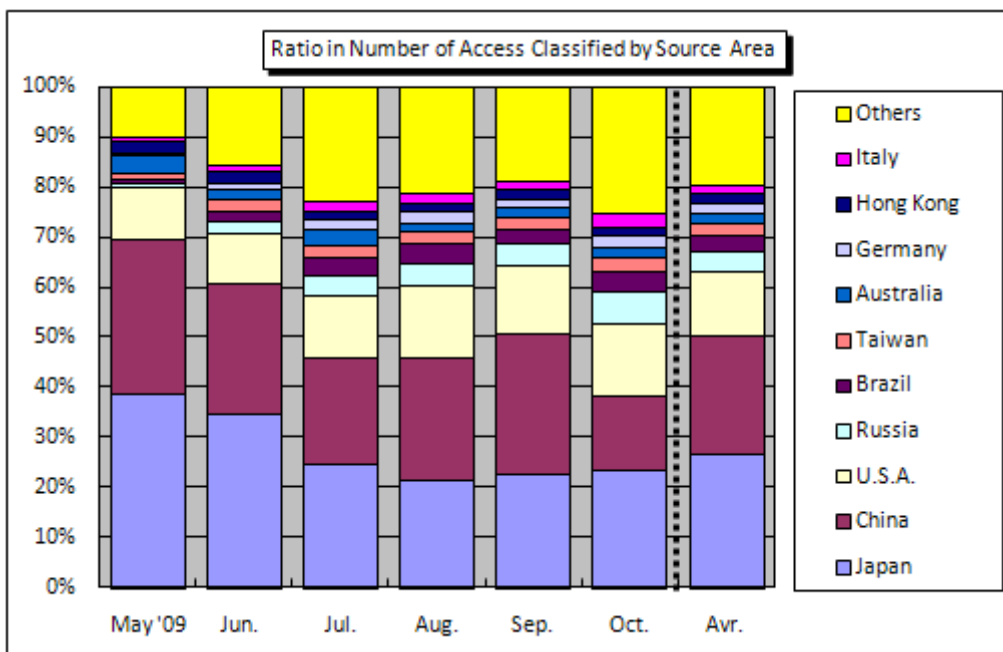
**Chart 3-1: Ratio in Number of Access Classified by Destination (by Port) from May to October 2009**



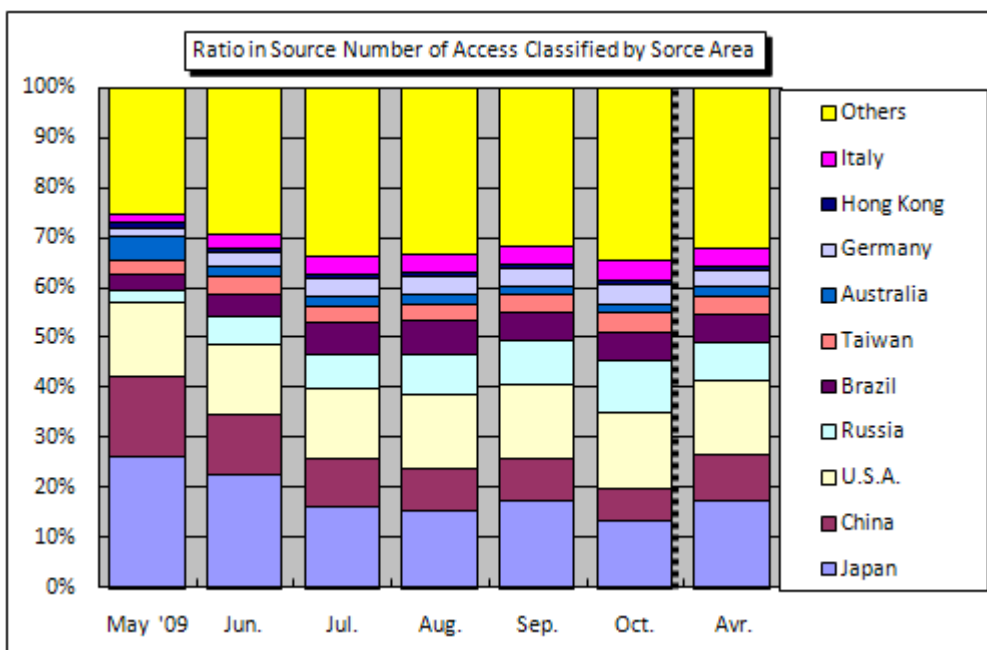
**Chart 3-2: Ratio in Source Number of Access Classified by Destination (by Port) From May to October 2009**

**(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 May to October 2009.



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



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

#### 4. Supplementary Explanations

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

Port Type	Interpretations/Descriptions
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.
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.
2967/tcp	High potential of access which targets vulnerability in Symantec products such as Symantec Client Security and Symantec AntiVirus, etc.
1434/tcp	Renowned by unauthorized computer access targeting the vulnerability (by W32/SQL Slammer) in Microsoft SQL Server, etc.
139/tcp	Renowned by unauthorized computer access targeting the file (network) sharing for which security is insufficient; this port is frequently targeted by those accesses which target vulnerability in Windows.
5900/tcp	This seems to be the access which targets vulnerability in RealVNC, the one of remote accessing tools.
4899/tcp	Renowned by unauthorized computer access which targets to the vulnerability in RAdmin for remote operation (RAdmin is the application which enables to operate multiple computers remotely).

**Inquiries to:**

Information-Technology Promotion Agency, Security Center  
 Oura/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)