

## Report from the Internet Monitoring (TALOT2)

January 2009

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

In the Internet Monitoring (TALOT2), unwanted (one-sided) access in January totaled **131,296** cases for the 10 monitoring points and the gross number of the sources\* was **41,171**: unwanted (one-sided) access captured at one monitoring point was about **424** accesses from about **132** sources per day.

**Gross Number of Source (\*):** The gross number of the source being accessed to the 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.

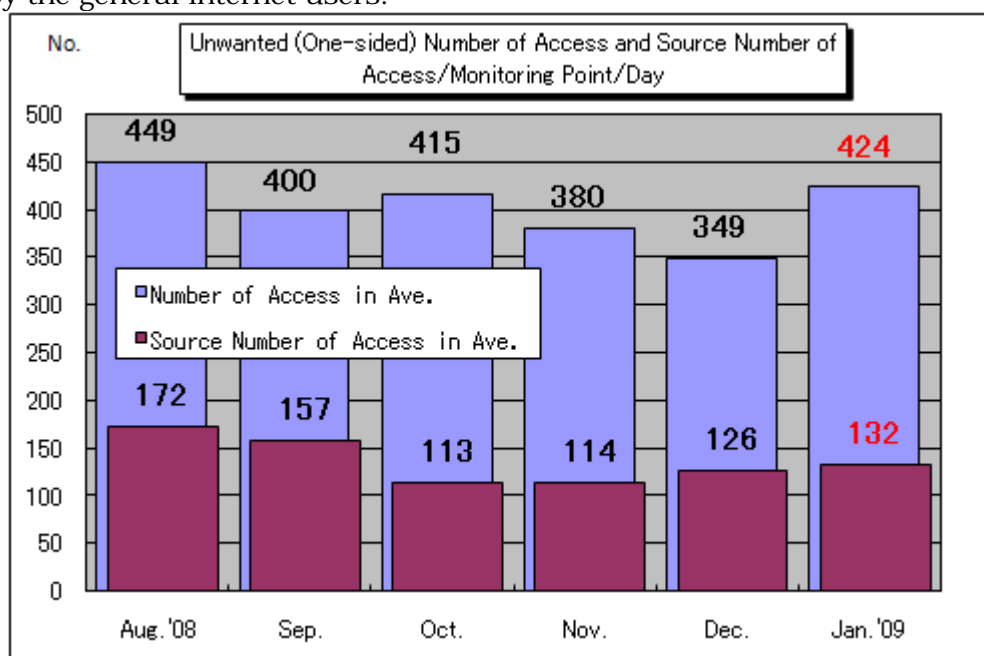


Chart 1-1: Unwanted (One-sided) Number of Access and Source Number of Access/Monitoring Point/Day

The Chart 1-1 shows the unwanted (one-sided) number of access (average) and the source number of access (average)/monitoring point/day from August 2008 to January 2009. Both unwanted (one-sided) number of accesses (average) in January 2009 were increased compared with the one in December 2008.

The Chart 1-2 shows the comparison of number of accesses in December 2008 and in January 2009. The number of access to the ports 445/tcp and 135/tcp were the significantly increased in January: These ports have high potential to get targeted by the attack which exploits vulnerability in Windows. The cause of access increase to the port 445/tcp will be described in the following section.

For your further information, the access increase to the port 135/tcp has not yet clarified, however, we have to be cautious and to continually watch it for.

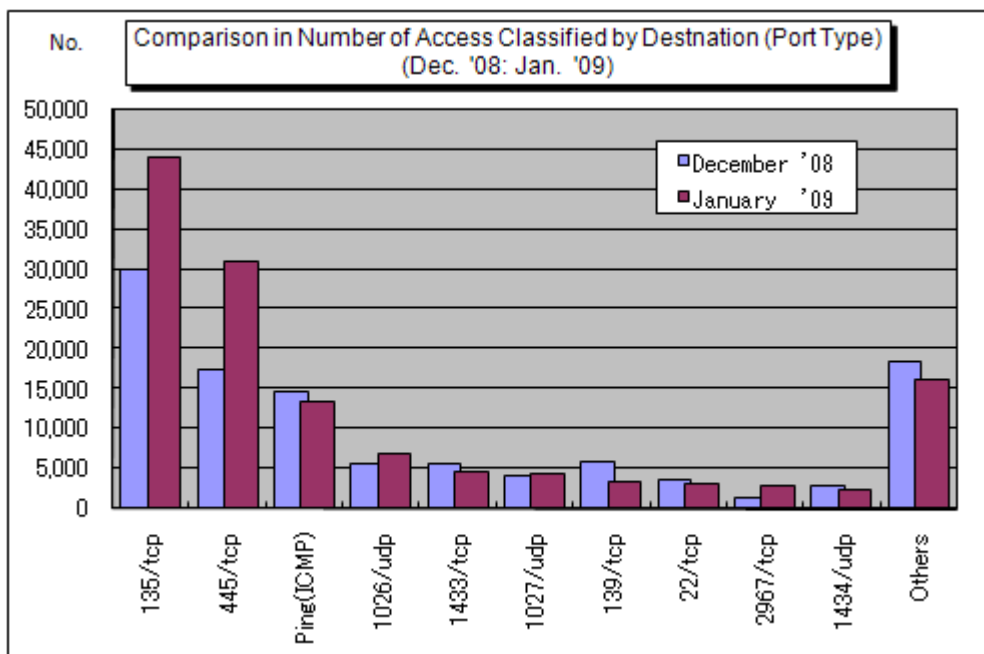


Chart 1-2: Comparison in Number of Access Classified by Destination (by Port) (Dec. 08/Jan. 09)

## 2. The Peculiar Access in January 2009

### (1) Access to the Port 445/tcp

The Chart 2-1 shows the shift in number of access to the port 445/tcp from October 2008 to January 2009. As we already reported the access increase to the port 445/tcp in the December report, the tendency was getting further remarkable in January 2009.

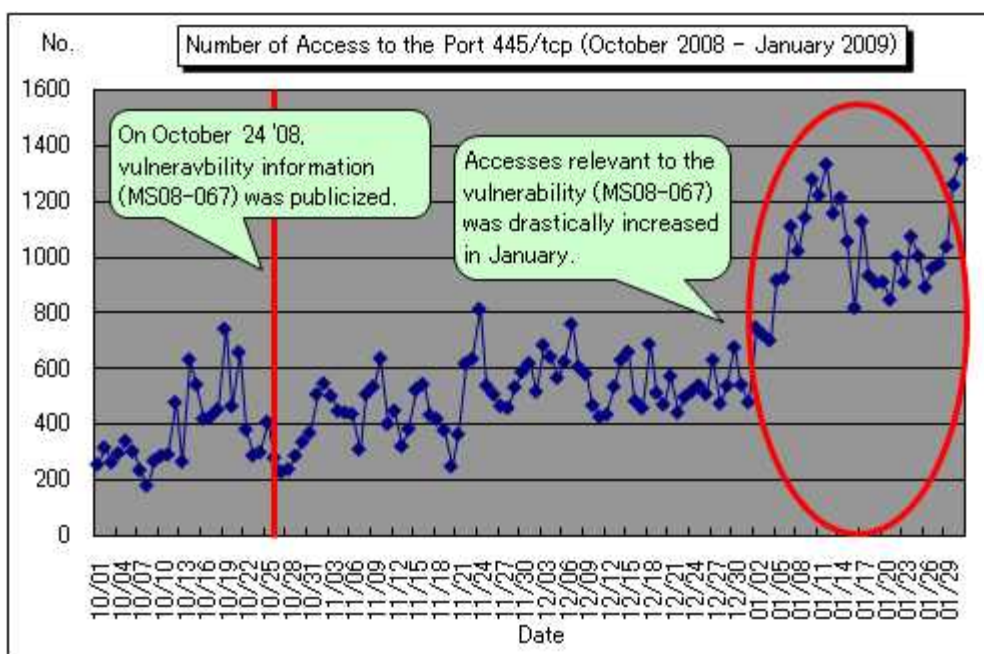


Chart 2-1: Number of Access to the Port 445/tcp (Total for 10 Monitoring Points)

This may be the access which targeted the vulnerability (MS08-067) in Windows which emergently publicized from Microsoft in October 24, 2008 (Japan time). According to Microsoft, such accesses to the port, i.e., attacks which exploits this vulnerability, was identified about 2 weeks ago when the information was publicized by Microsoft. This access mainly targeted Windows series of servers, and Windows computers for general users.

This vulnerability allows to execute arbitrary commands unintentionally when specially crafted packet (communication data) was sent to targeted computer which renders the services to share file (s) and printer (s) in Windows.

## &lt;Reference&gt;

Microsoft Security Bulletin MS08-067 - Critical Vulnerability in server service could allow remote code execution

<http://www.microsoft.com/technet/security/bulletin/MS08-067.mspx>

“What is the Vulnerability (MS08-067) in Windows” (IPA) (in Japanese)

<http://www.ipa.go.jp/security/ciadr/vul/20081024-ms08-067.html>

There identified the virus so called Downadup which conducts the attack exploiting this vulnerability. This virus was initially detected in the end of November 2008, and then, its variant so called Downadup.B was detected in the end of December 2008. This virus initially infects to the computer via the Internet for which vulnerability has not yet been resolved: then the virus attempts infection activities to the other computers based on the computer initially infected. Accordingly, even single computer is infected in a LAN environment in where number of computers are connected, the infection will be enlarged within that LAN environment in that business/organization, school, etc.

For your information, Downadup.B, the variant of Downadup, additionally features to infect to outside memory media such as USB memory, etc. The drastic access increase to the port 445/tcp in January may be the cause that **some user may have been connected to the USB memory to the computer in the LAN environment in his/her business/organization that have been already infected by the virus at his/her home computer**. The emergence of the virus variant, those computers infected by virus was increased and each of them attacked the other computers respectively that led this drastic access increase.

Since the fundamental and mandatory measures to prevent damage by the virus is to resolve vulnerability in your computer; accordingly, be sure to check your computer if any of vulnerabilities in your computer is adequately resolved or not one more time. If they are not, please apply latest security patches to resolve them NOW!

## &lt;Reference&gt;

“Microsoft Update helps keep your computer current”(Microsoft)

<http://www.microsoft.com/protect/computer/updates/mu.mspx>

**(2) Access to the Port 80/tcp**

Though the access to the port 80/tcp was not ranked in the worst 10 for the number of access classified by destination (port type) in January, it had been drastically increased in a short period of time (average before January 8 was 22/day for a week: at the peak period was 414/day for a week).

This access increase to the port 80/tcp was drastically increased on January 8, and then it got clam down within several days (See the Chart 2-2).

This symptom was monitored in all 10 monitoring points in TALOT2 system simultaneously (See the Chart 2-3): Since the same symptom was also monitored in the other Internet monitoring systems provided by different organizations, it can be assumed that this access increase may be generated in relatively broad area range at the same timing.

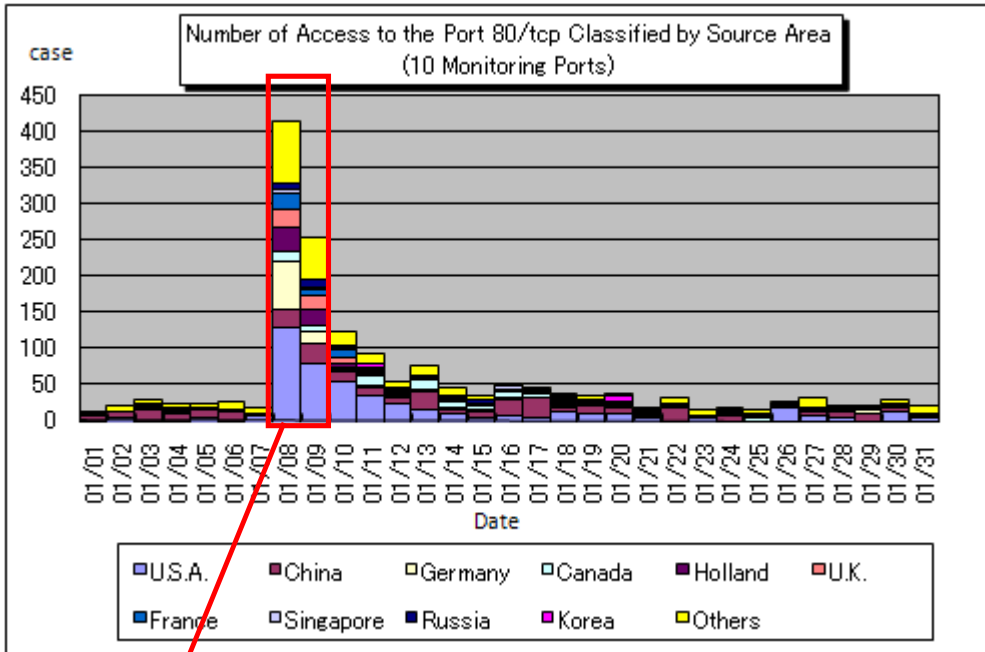


Chart 2-2: Number of Access to the Port 80/tcp Classified by Source Area (10 Monitoring Points)

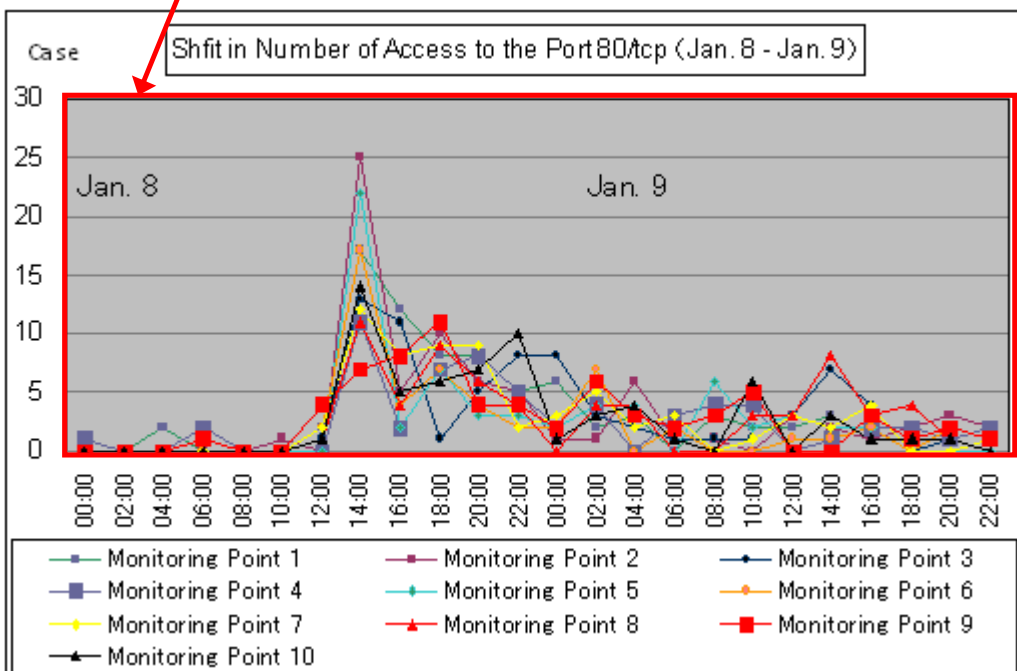


Chart 2-3: Number of Access to the Port 80/tcp Classified by Monitoring Point (Jan. 8/Jan. 9)

In addition, MUSTAN (\*), the other Internet monitoring system in IPA also monitored same symptom. There identified following letter string in its access logs.

```
/nonexistenshit  
/mail/bin/msgimport  
/bin/msgimport  
/rc/bin/msgimport  
/roundcube/bin/msgimport  
/webmail/bin/msgimport
```

The “msgimport” file above may be related to the web mail software so called “Roundcube Webmail”. The access may have searched the server for which vulnerability had not yet been resolved as its security patches was just released in the middle of December 2008.

#### <Reference>

Vulnerability Information for “RoundCube Webmail” (SOURCEFORGE.NET)

[http://www.sourceforge.net/forum/forum.php?forum\\_id=898542](http://www.sourceforge.net/forum/forum.php?forum_id=898542)

Release Information for “RoundCube Webmail” (SOURCEFORGE.NET)

[http://www.sourceforge.net/forum/forum.php?forum\\_id=902703](http://www.sourceforge.net/forum/forum.php?forum_id=902703)

It may cause such damage that your privacy (information) is violated or your confidential information is leaked when intruded by the mail system such as “Roundcube Webmail”, etc. Accordingly, those system administrators who use “Roundcube Webmail” should upgrade your mail system to the latest stabled version by referring the URLs above.

Since vulnerability (information) is publicized, such access relevant to that vulnerability may be increased in a short period of time. Accordingly, be sure to be ready to resolve any of vulnerabilities involved with your computer. To that end, it is helpful to check the vulnerability information supporting site such as JVN, etc. daily.

MUSTAN (\*): MUSTAN (MULTi Sensor Traffic ANalysis) refers the system which provide the information relevant to aggressive traffic by monitoring/analyzing them on the Internet by the sensors allocated on number of monitoring points.

#### <Reference>

“MUSTAN Internet Report” (in Japanese)

[http://mustan.ipa.go.jp/mustan\\_web/](http://mustan.ipa.go.jp/mustan_web/)

“JVN (Japan Vulnerability Notes)” (in Japanese)

<http://jvn.jp/>

“JVN iPedia, the Database for Vulnerability Measures Information”

<http://jvndb.jvn.jp/>

### 3. One-sided Accesses in January 2009

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

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 January 2009.

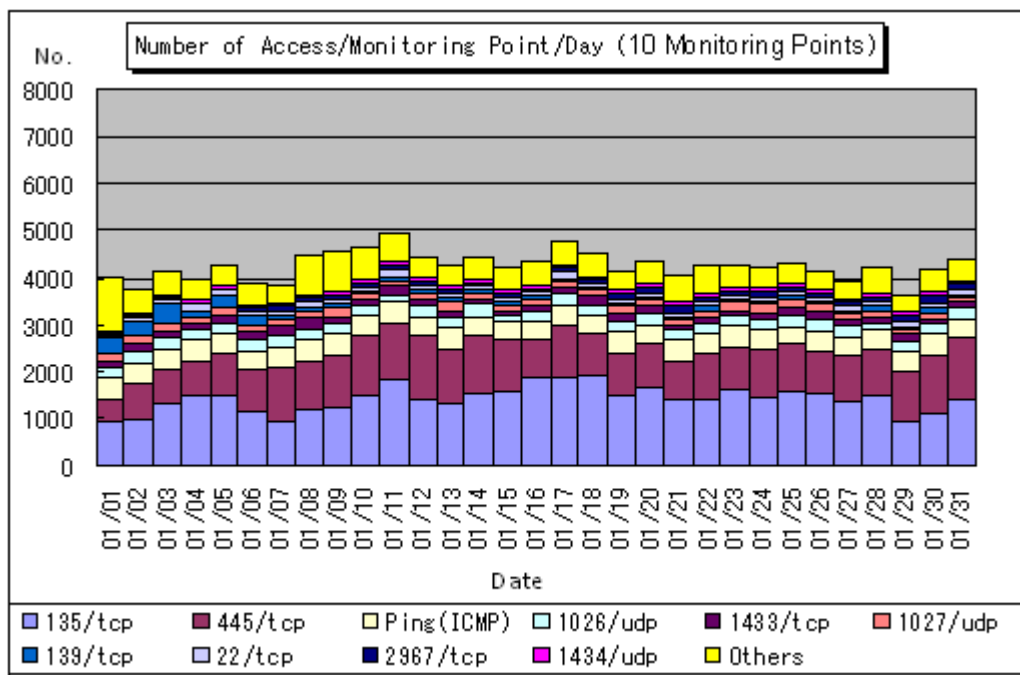


Chart 3-1: Number of Access/Monitoring Point/Day in January 2009

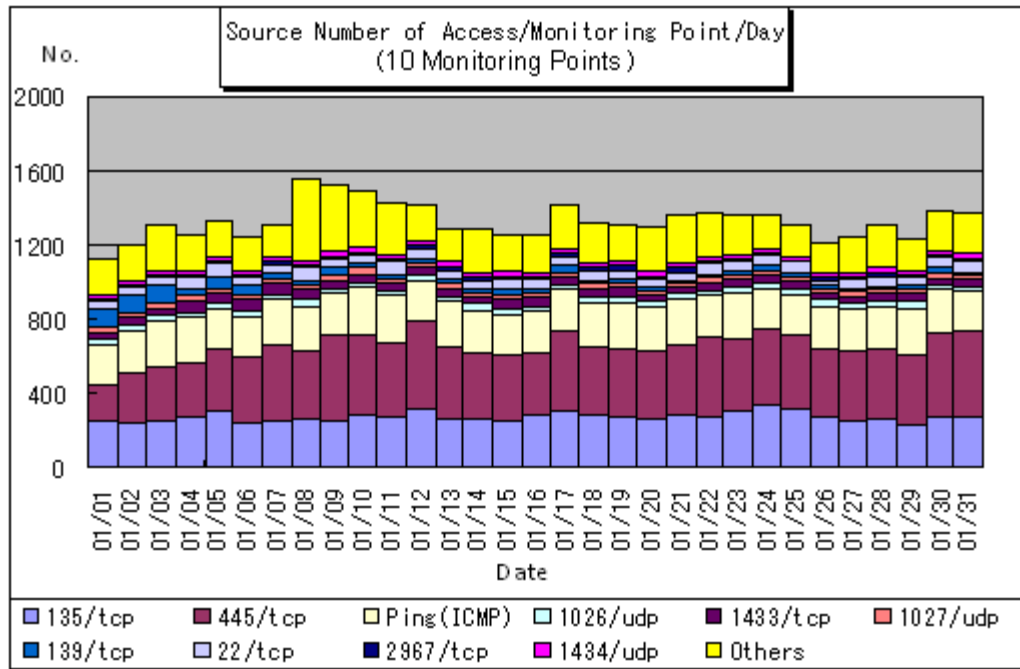


Chart 3-2: Source Number of Access/Monitoring Point/Day in January 2009

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

The Chart 3-3 shows the ratio in number of access classified by destination (port type) and the Chart 3-4 shows the ratio in source number of access classified by destination (port type) in January 2009. For your information, respective ratios are rounded at the 1<sup>st</sup> arithmetic point; accordingly, it may not make 100% sharp.

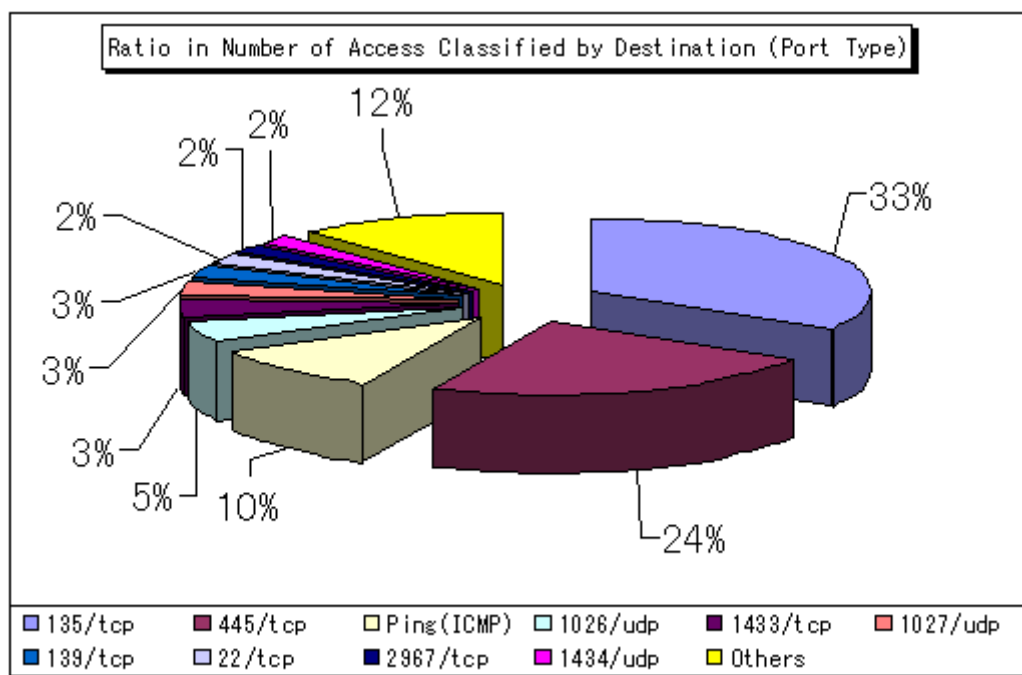


Chart 3-3: Ratio in Number of Access Classified by Destination (Port Type) in January 2009

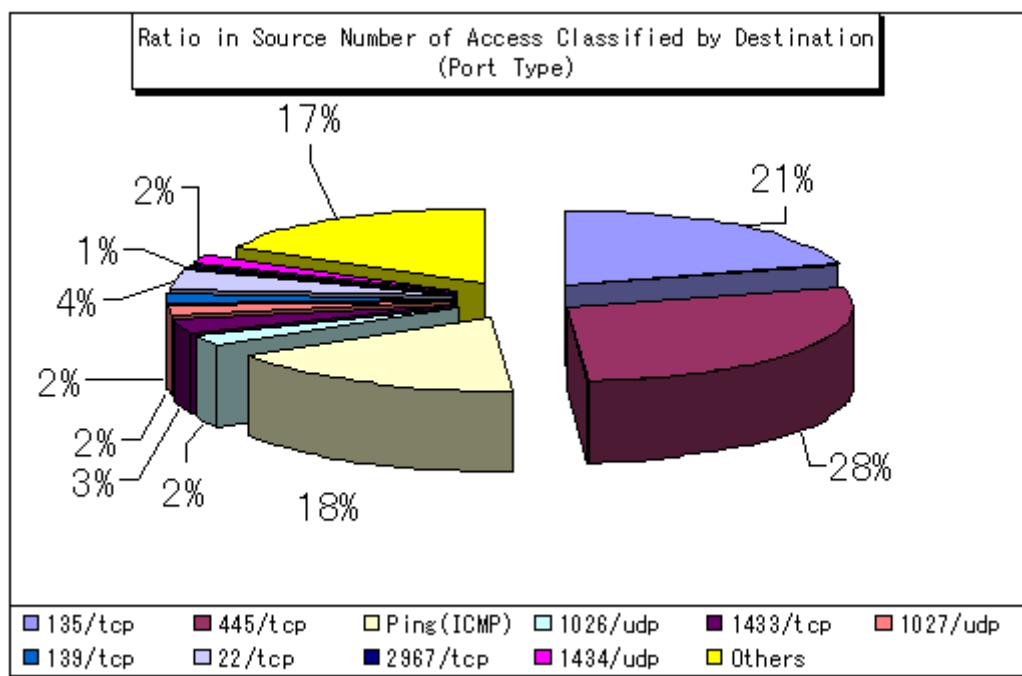


Chart 3-4: Ratio in Source Number of Access Classified by Destination (Port Type) in January 2009

**(3) Accesses Classified by Source Area**

The Chart 3-5 shows the shift in number of access classified by source area and the Chart 3-6 shows the ratio in number of access classified by source area in January 2009. For your information, ratios are rounded at the 1<sup>st</sup> arithmetic point; accordingly, it may not make 100% sharp.

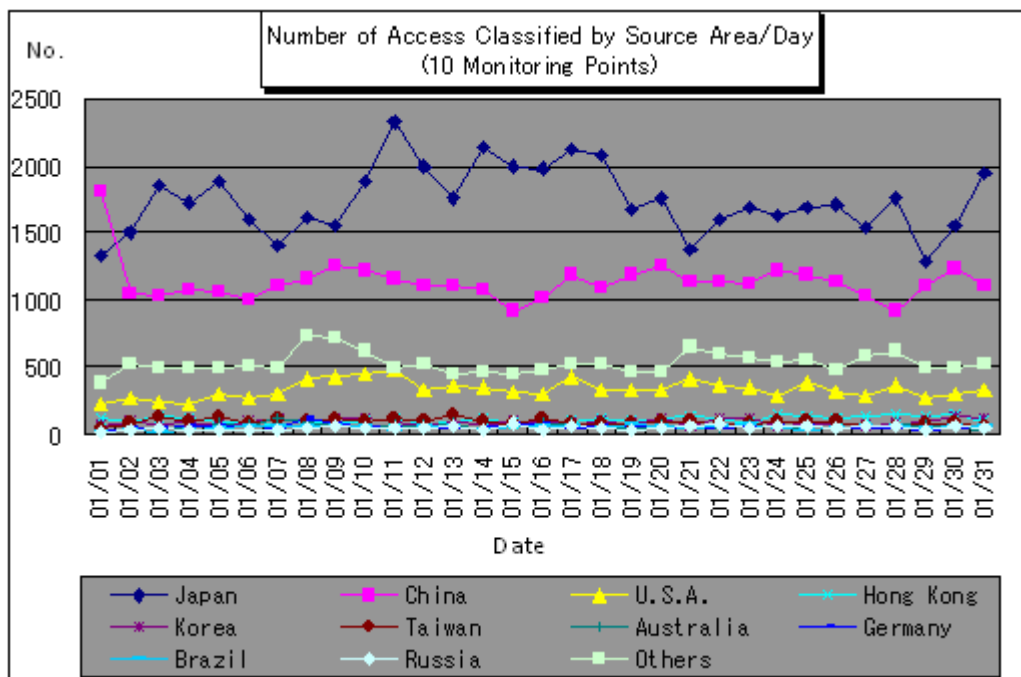


Chart 3-5: Number of Access Classified by Source Area/Day in January 2009

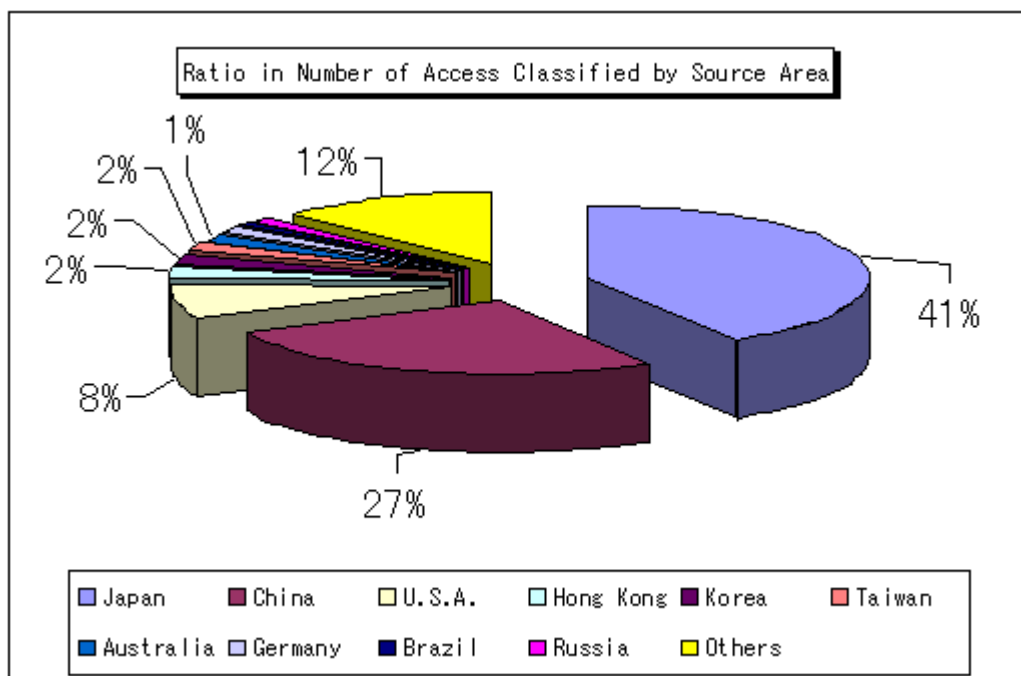


Chart 3-6: Ratio in Number of Access Classified by Source Area in January 2009

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 January 2009. For your information, ratios are rounded at the 1<sup>st</sup> arithmetic point; accordingly, they may not make 100% sharp.

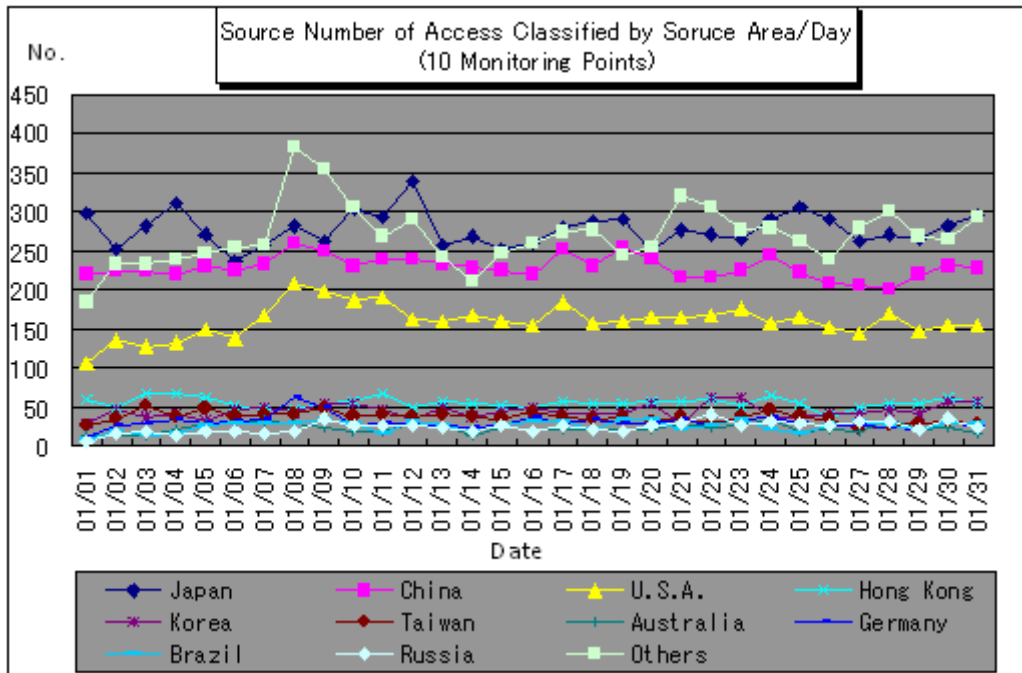


Chart 3-7: Source Number of Access Classified by Source Area/Day in January 2009

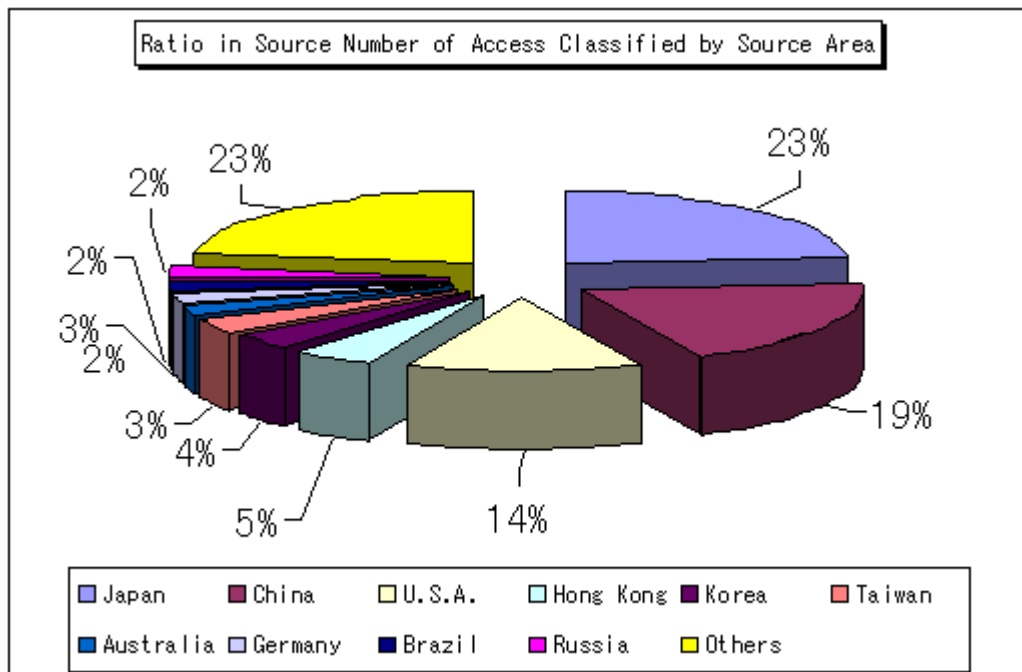


Chart 3-8: Ratio in Source Number of Access Classified by Source Area in January 2009

4. Statistic Information

(1) Ratio Classified by Destination (Port Type)

The Chart 4-1 shows the ratio in number of access classified by destination (port type) and the Chart 4-2 shows the ratio in source number of access classified by destination (port type) in January 2009.

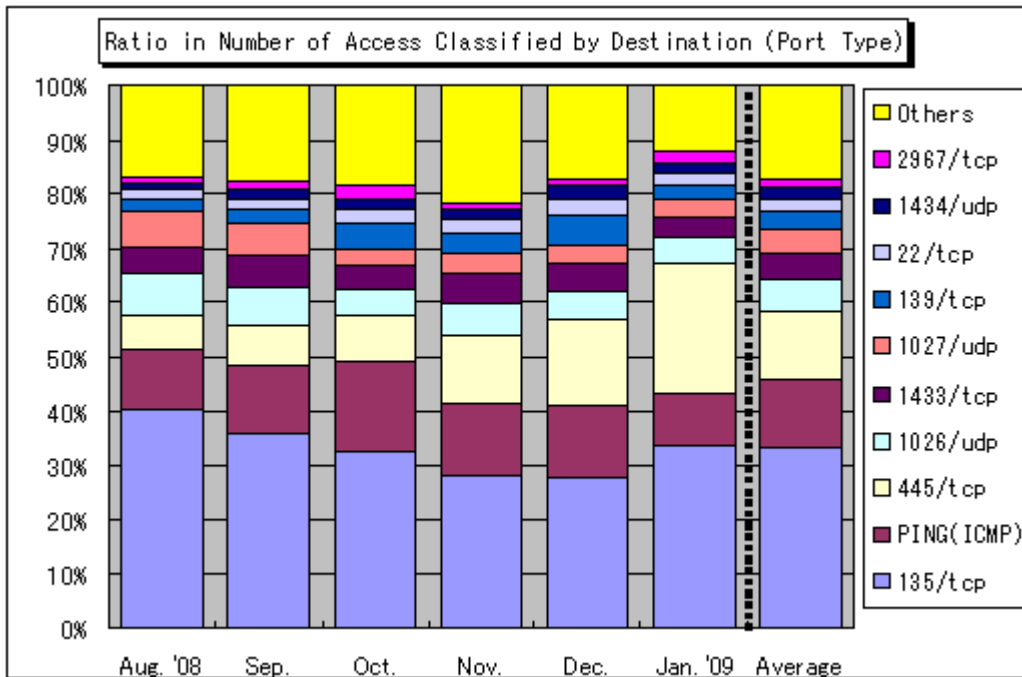


Chart 4-1: Ratio in Number of Access Classified by Destination (Port Type) from August 2008 to January 2009

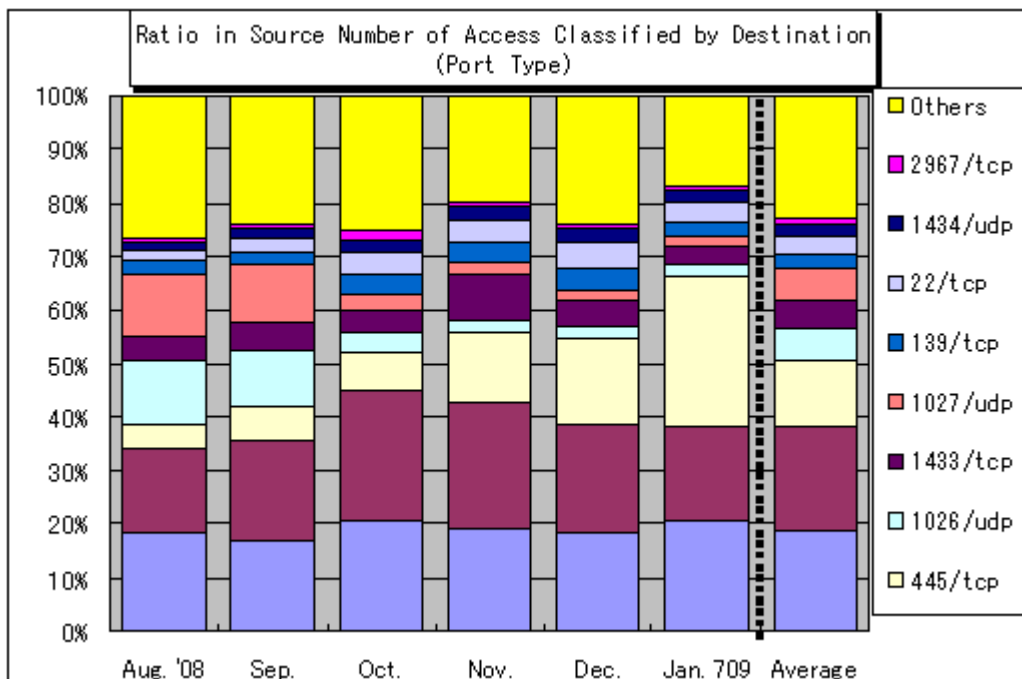


Chart 4-2: Ratio in Source Number of Access Classified by Destination (Port Type) from August 2008 to January 2009

**(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 August 2008 to January 2009.

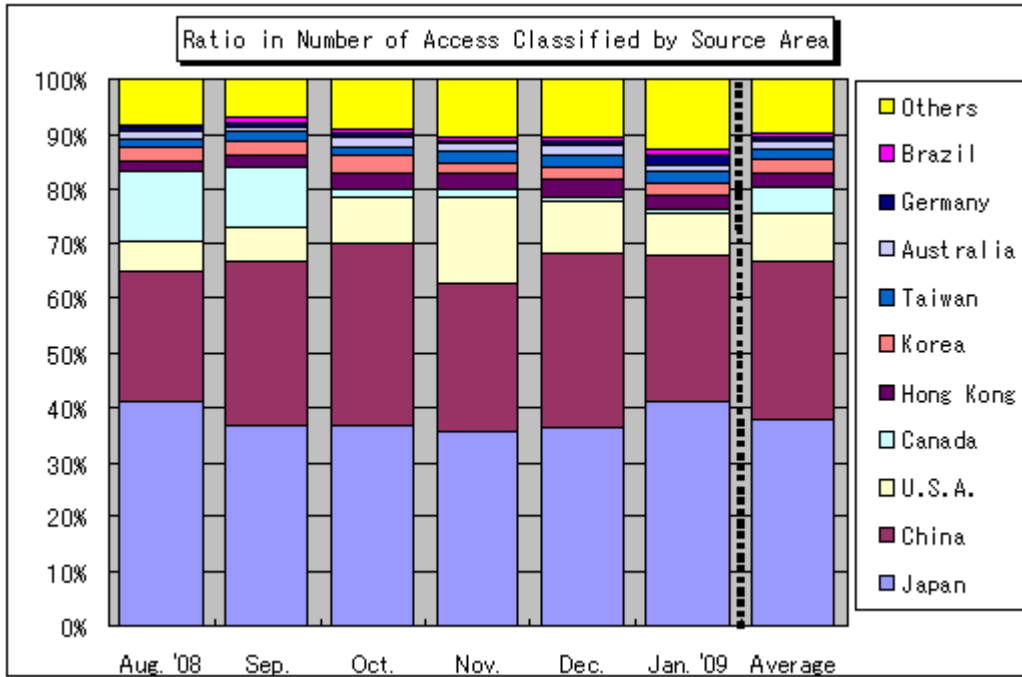


Chart 4-3: Ratio in Number of Access Classified by Source Area from August 2008 to January 2009

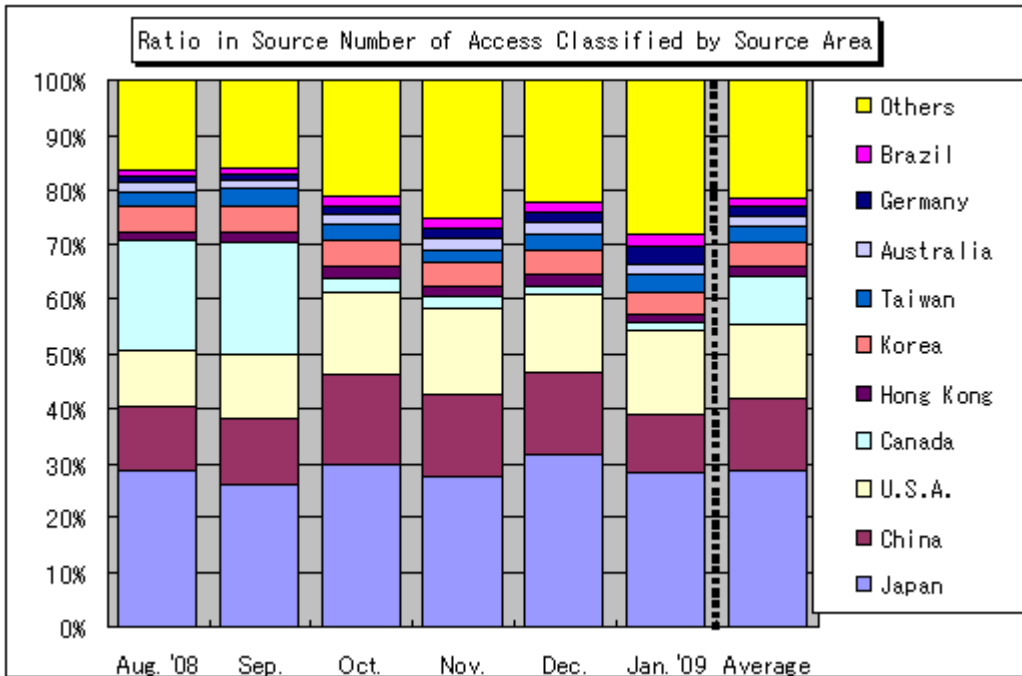


Chart 4-4: Ratio in Source Number of Access Classified by Source Area from August 2008 to January 2009

## 5. Supplementary Explanations

Following are the explanations for the destination (port type) remarkably accessed (either in-bound or out-bound or both) in January 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, 1028/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.
1434/udp	Renowned for the fraudulent access, etc. targeting vulnerability in Microsoft SQL Server (W32/SQLSlammer, etc.).
2967/tcp	High potential of access which targets vulnerability in Symantec products.

***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)