

## Report from the Internet Monitoring (TALOT2)

February 2009

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

In the Internet Monitoring (TALOT2), unwanted (one-sided) access in January totaled **138,944** cases for the 10 monitoring points and the gross number of the sources\* was **48,671**: unwanted (one-sided) access captured at one monitoring point was about **579** accesses from about **203** 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.

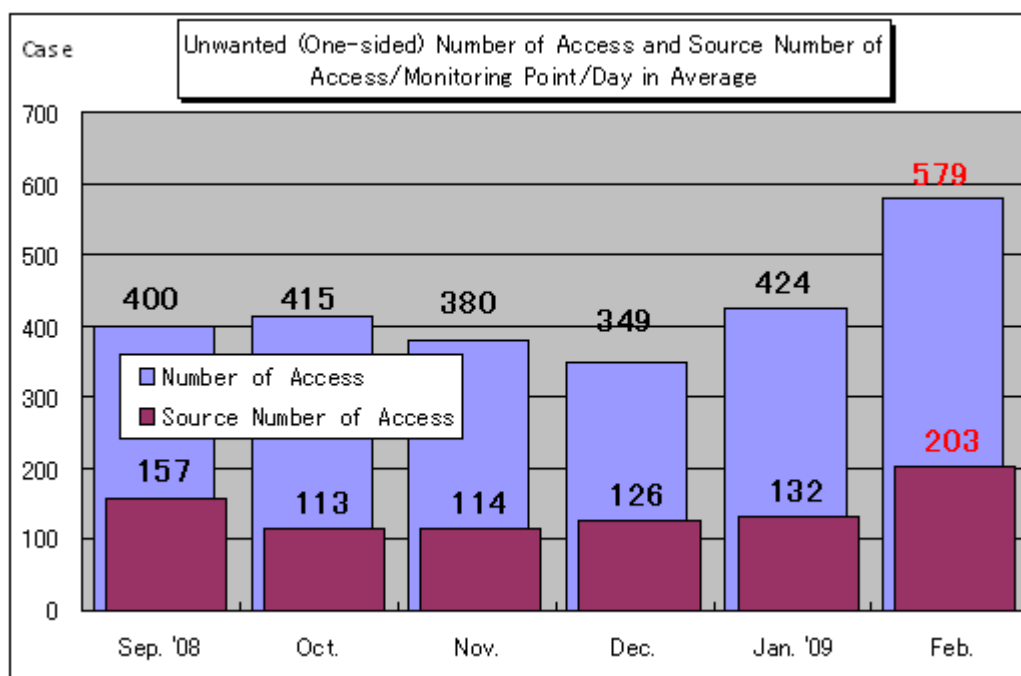


Chart 1-1: Unwanted (One-sided) Number of Access (Average) and Source Number of Access (Average)/Monitoring Point/Day

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

The Chart 1-2 shows the comparison of number of access classified by destination (by port) for January and February. The port the number of access was drastically increased compared with the one in January was 445/tcp. The access to the port 445/tcp was drastically increased after the system maintenance period, from February 6 to 9. For further details, please refer to the (2) of II (Access to the Port 445/tcp in Peculiar Access in February 2009.). This port has high potential to be targeted by the attack which targets to vulnerability in Windows.

In addition, the access to the port 21897/tcp, the none-accessed port in January, was remarkably monitored. The purpose of this access has not yet been analyzed: however, it may be the access attempting to re-connect to the IP address being used by a file sharing software as this access was only monitored at a single monitoring point on a specific day. The IP address previously allocated to the file sharing software in the other computer may incidentally allocate to the one of IP addresses for TALOT2 because of the system halt for maintenance.

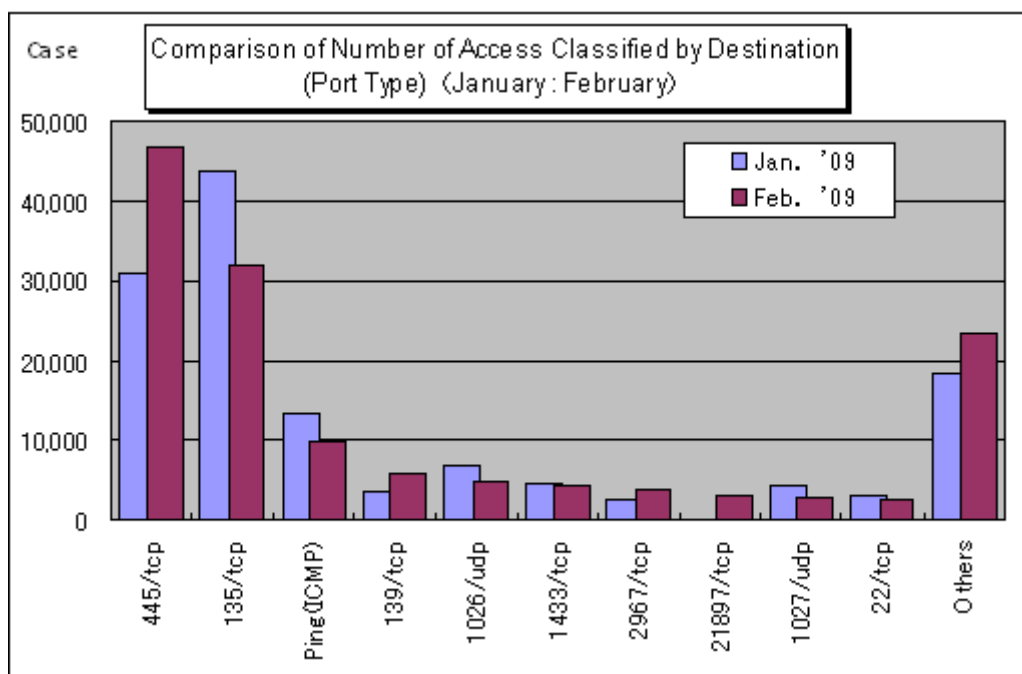


Chart 1-2: Comparison in Number of Access Classified by Destination (Port Type) (Jan. 09/Feb. 09)

## II. Peculiar Access in February 2009

### (1) The Access to 2967/tcp

The access to the port 2967/tcp increased from early part of January was remarkably increased in February (See the Chart 2-1.).

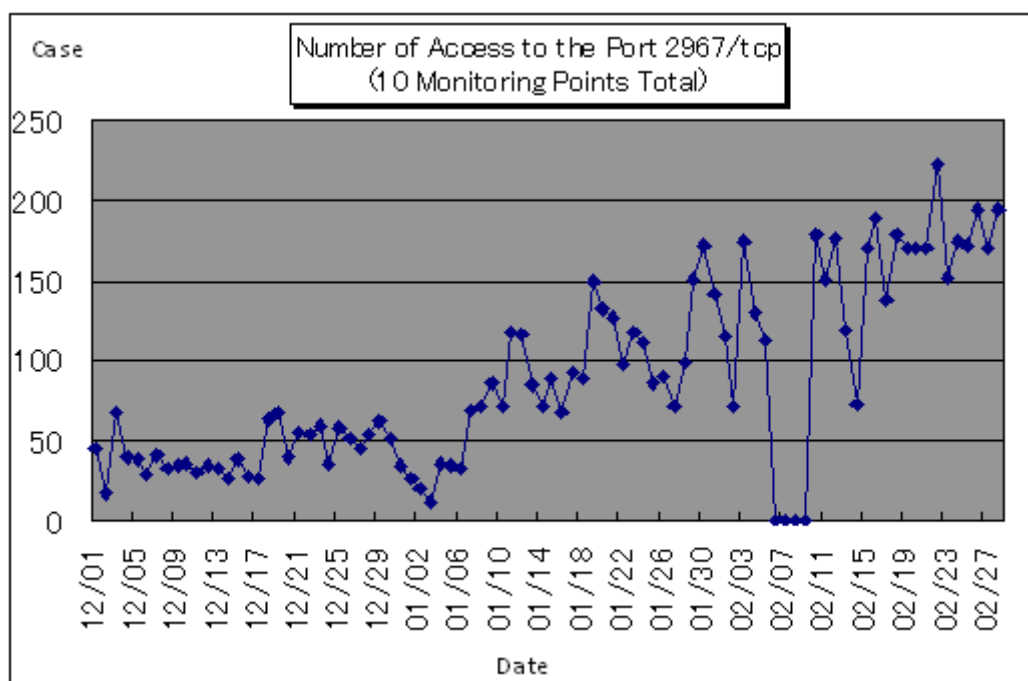


Chart 2-1: Number of Access to the Port 2967/tcp (10 Monitoring Points Total)

2967/tcp is the default port used by Symantec products. The vulnerability relevant to "Symantec Client Security and Symantec AntiVirus which allow privilege escalation (SYM06-010) was publicized in the past.

This vulnerability allows malicious attackers gain/delete specific files in the targeted products such as Symantec Client Security and Symantec AntiVirus, etc. so that they will be no longer available for use (i.e., will be destructed).

## &lt;Reference&gt;

Vulnerability allowing “Symantec Client Security and Symantec AntiVirus Elevation Privilege (SYM06-010)” (Publicized on May 25, 2006)

<http://www.symantec.com/avcenter/security/Content/2006.05.25.html>

It is probable that the attack targeting this vulnerability is conducted up to current. However, those Symantec Client Security and Symantec AntiVirus users can resolve this vulnerability by updating their signature files utilizing Live Update session provided by Symantec. Accordingly, users should check whether your signature files are up-to-dated. If your supporting period is terminated and you cannot update your signature files, be sure to purchase/apply the latest version of signature files. Be sure to be ready to conduct anti-vulnerability measures for the products now you are using: to that end, it is necessary to check the portal sites relevant to vulnerability information such as JVN, etc. daily.

## &lt;Reference&gt;

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

<http://jvn.jp/>

“JVN iPedia - Database for anti-vulnerability measures” (in Japanese)

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

**(2) The Access to the Port 445/tcp**

Number of access to the port 445/tcp was already monitored in January; however, the access was getting further remarkable in February (See the Chart 2-2). As we described in the January report, the access to the port 445/tcp targeting the vulnerability in Windows for which information was emergently publicized by Microsoft in October 24, 2008 may still be remarkable.

## &lt;Reference&gt;

Internet Monitoring (TALOT2) for January 2009

<http://www.ipa.go.jp/security/english/virus/press/200901/documents/TALOT2-0901.pdf>

In the meantime, we analyzed the accessing status for the port before and after the system maintenance period (February 6 - 9), it is identified that the access from domestic was decreased, yet the access from overseas was significantly increased (See the Chart 2-3.).

One reason can be considered is the network segment for IP address was changed before and after the system maintenance period.

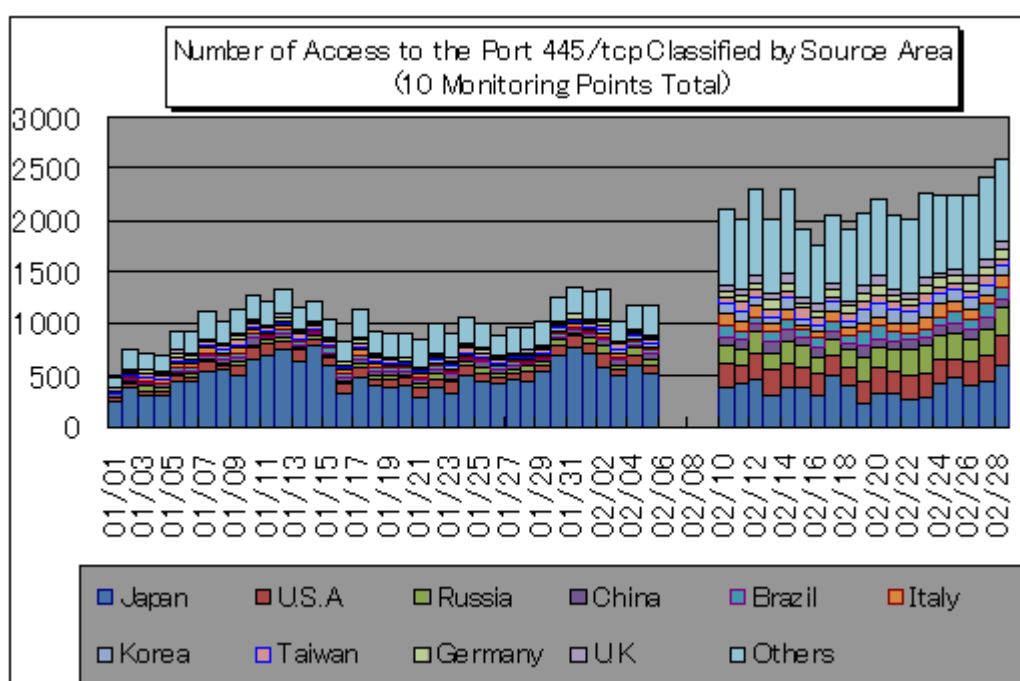


Chart 2-2: Number of Access to the Port 445/tcp Classified by Source Area

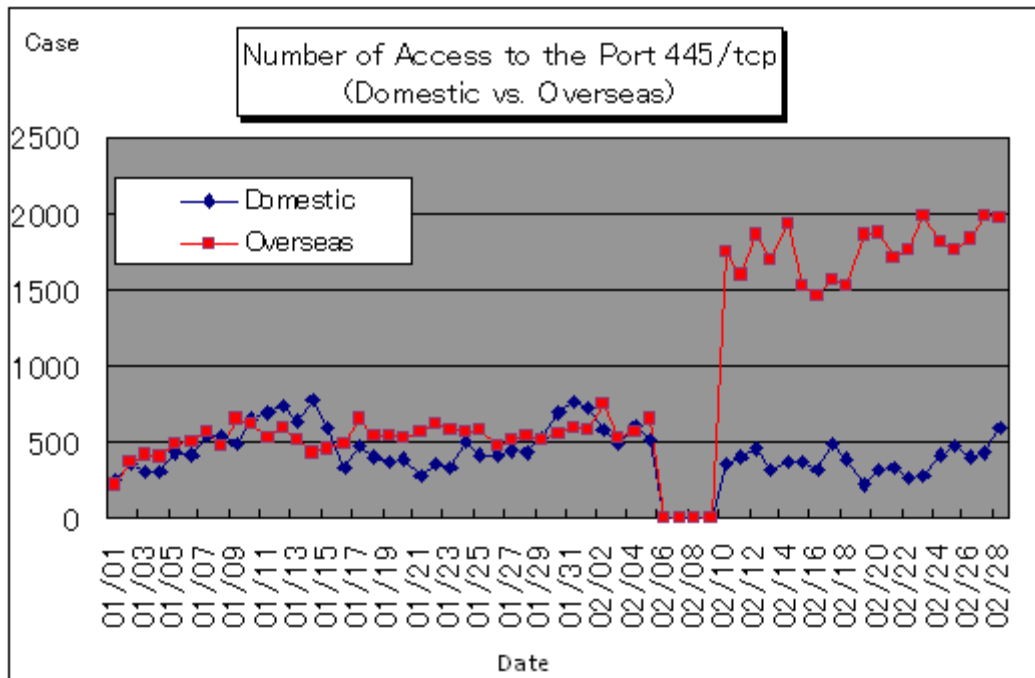


Chart 2-3: Number of Access to the Port 445/tcp (Domestic vs. Overseas)

### III. One-sided Accesses in February 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 February 2009.

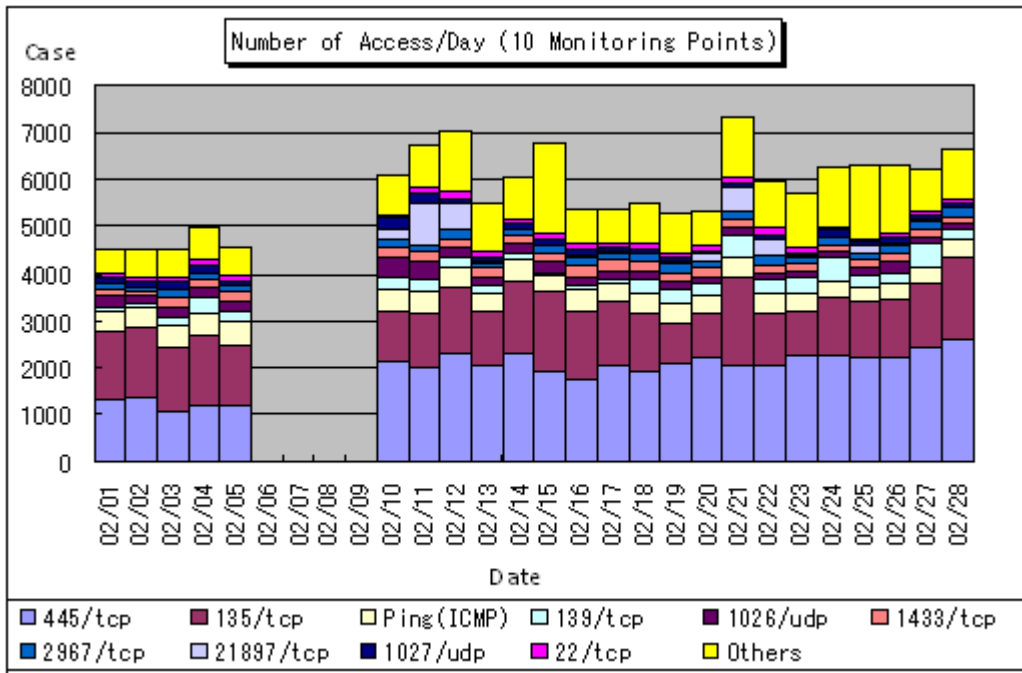


Chart 3-1: Number of Access/Day in February 2009

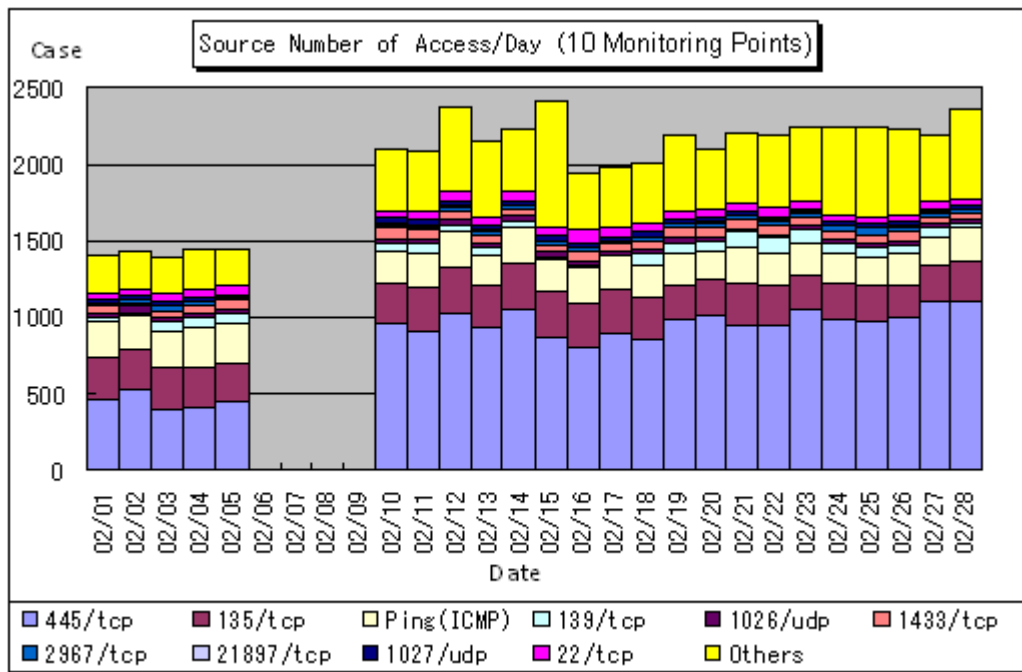


Chart 3-2: Source Number of Access/Day in February 2009

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

The Chart 3-3 shows the ratio in number of access classified by destination and the Chart 3-4 shows the ratio in source number of access classified by destination in February 2009. For your information, respective ratios are rounded at the 1<sup>st</sup> arithmetic point so that the total may not make 100% sharp, accordingly.

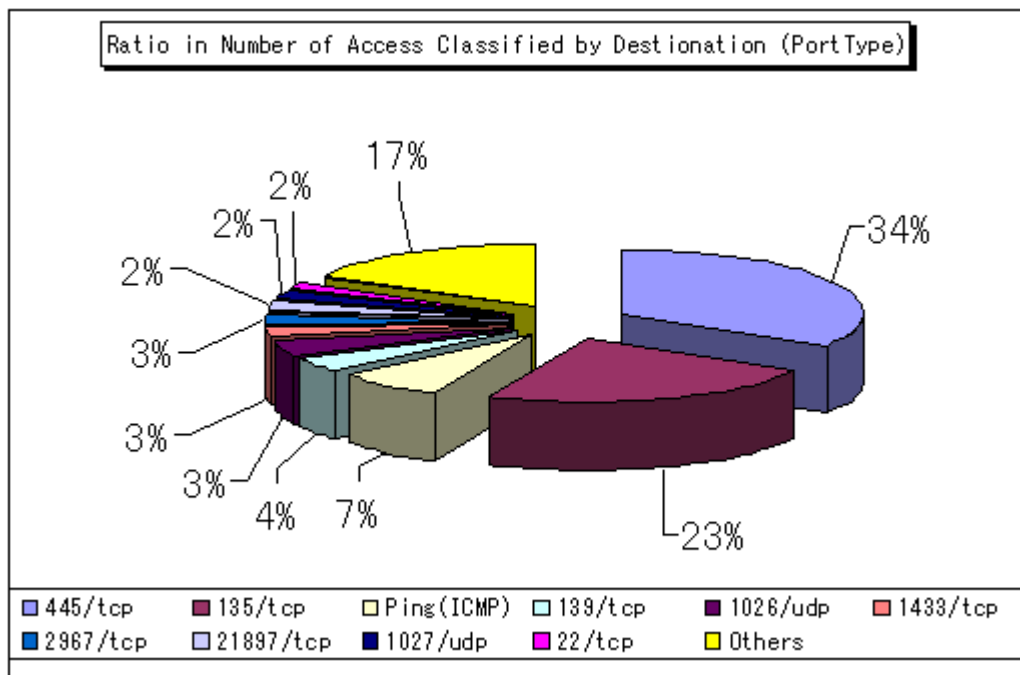


Chart 3-3: Ratio in Number of Access Classified by Destination (Port Type) in February 2009

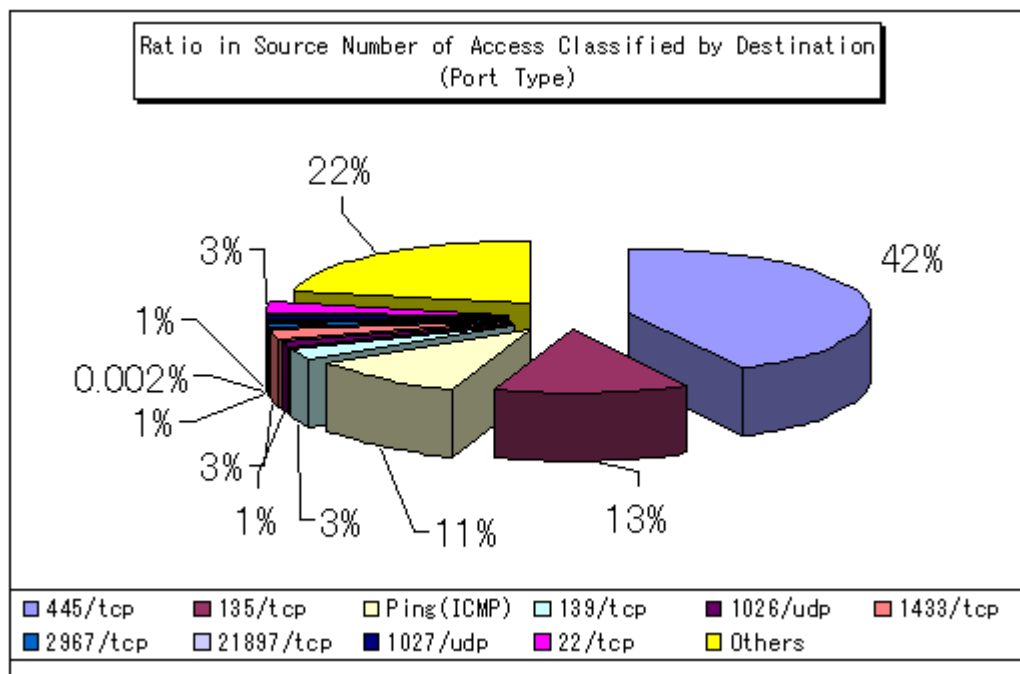


Chart 2-4: Ratio in Source Number of Access Classified by Destination (Port Type) in February 2009

(3) Accessing Status 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 February 2009. For your further information, respective ratios are rounded at the 1<sup>st</sup> arithmetic point so that it may not make 100% sharp, accordingly.

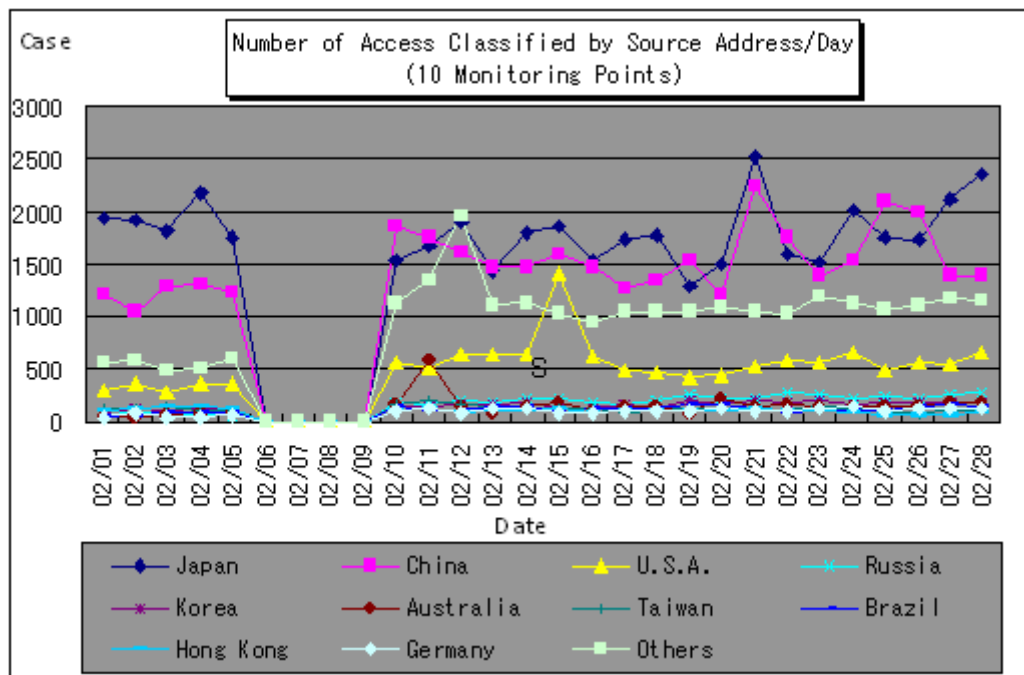


Chart 3-5: Number of Access Classified by Source Area/Day in February 2009

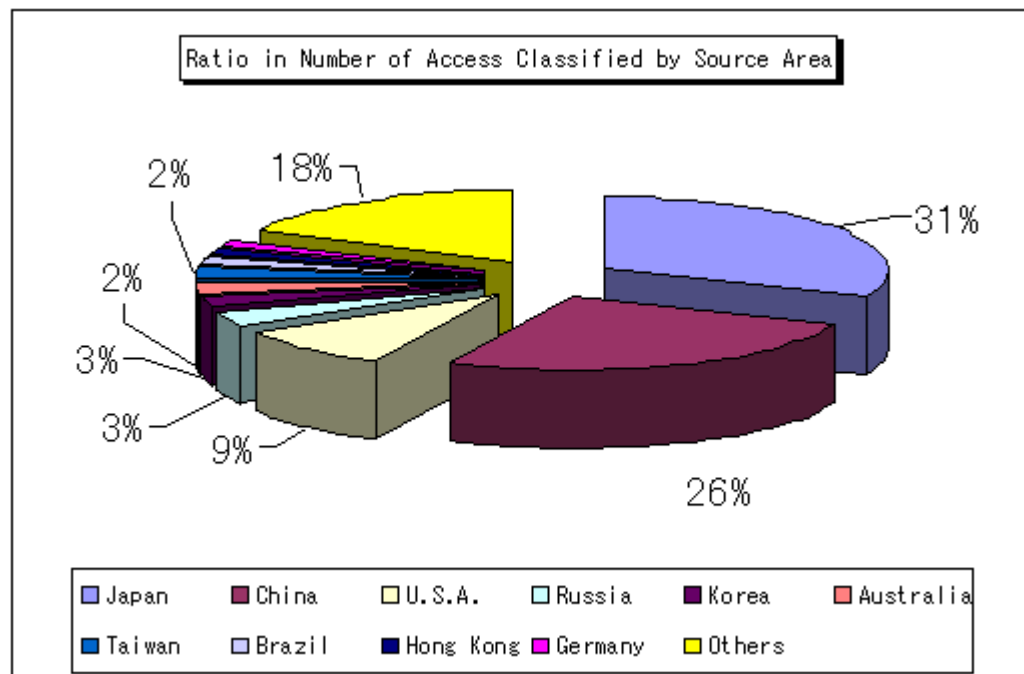


Chart 3-6: Ratio in Number of Access Classified by Source Area in February 2009

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. For your further information, the respective ratios are rounded at the 1<sup>st</sup> arithmetic point, so that it may not make 100% sharp, accordingly.

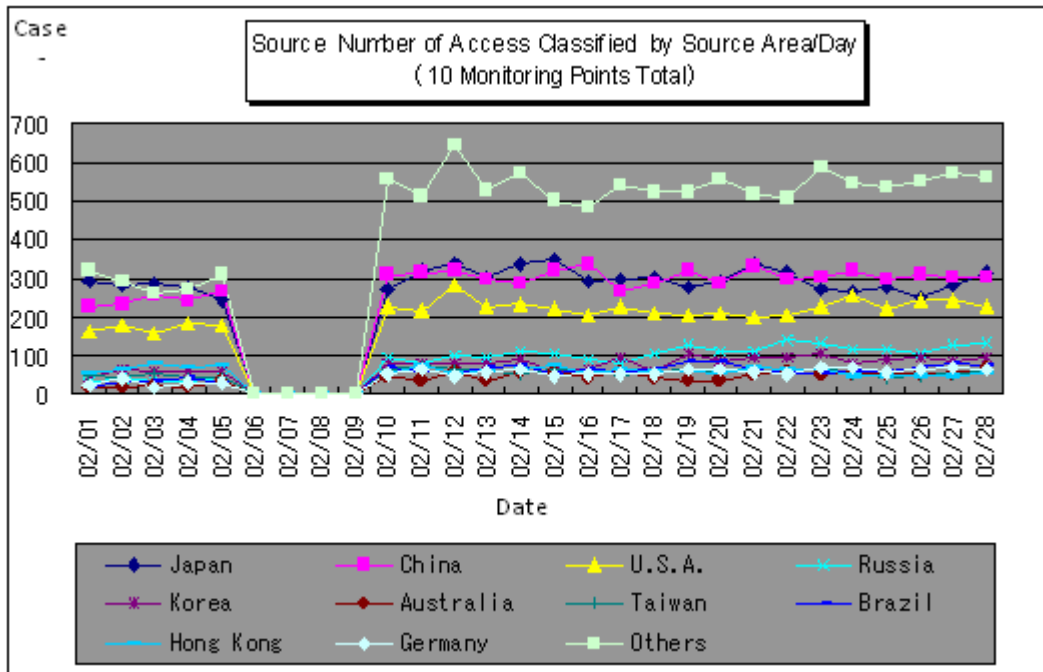


Chart 3-7: Source Number of Access Classified by Source Area/Day in February 2009

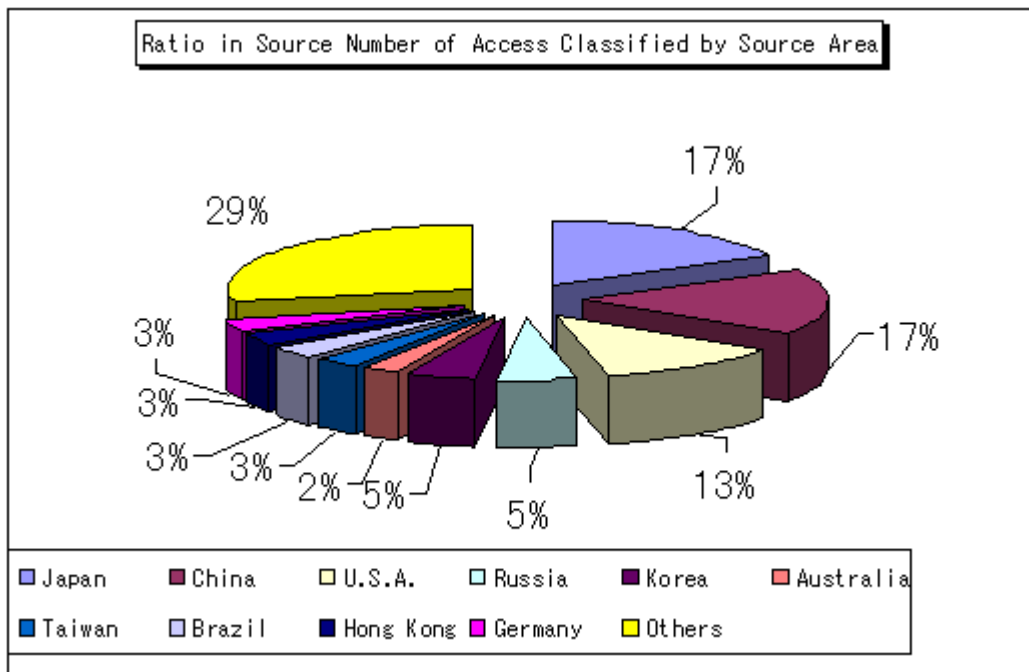
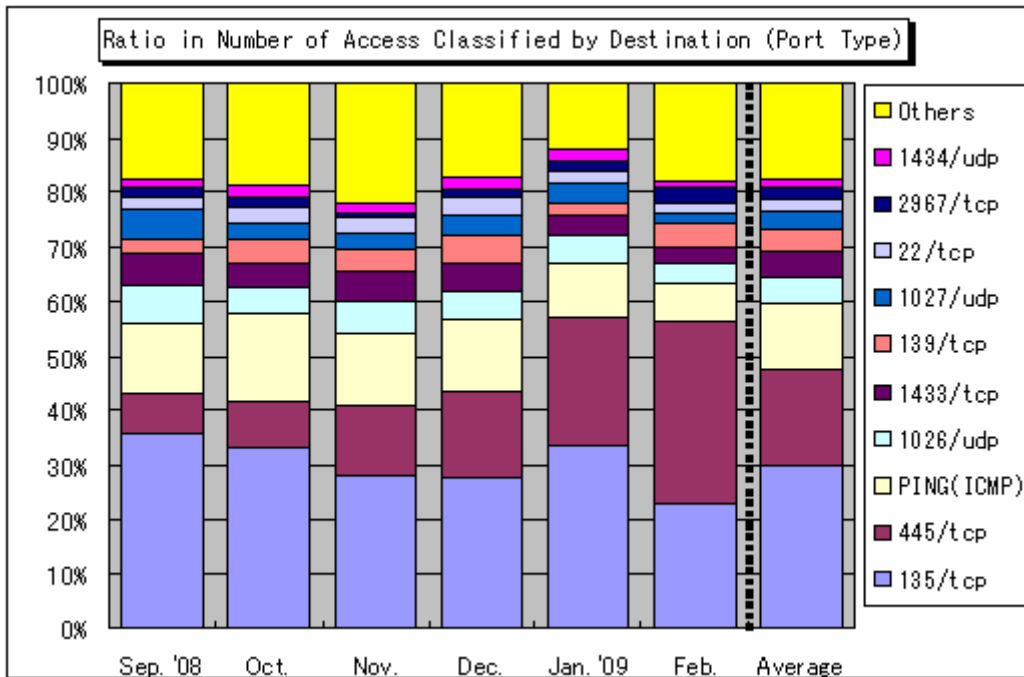


Chart 3-8: Ratio in Source Number of Access Classified by Source Area in February 2009

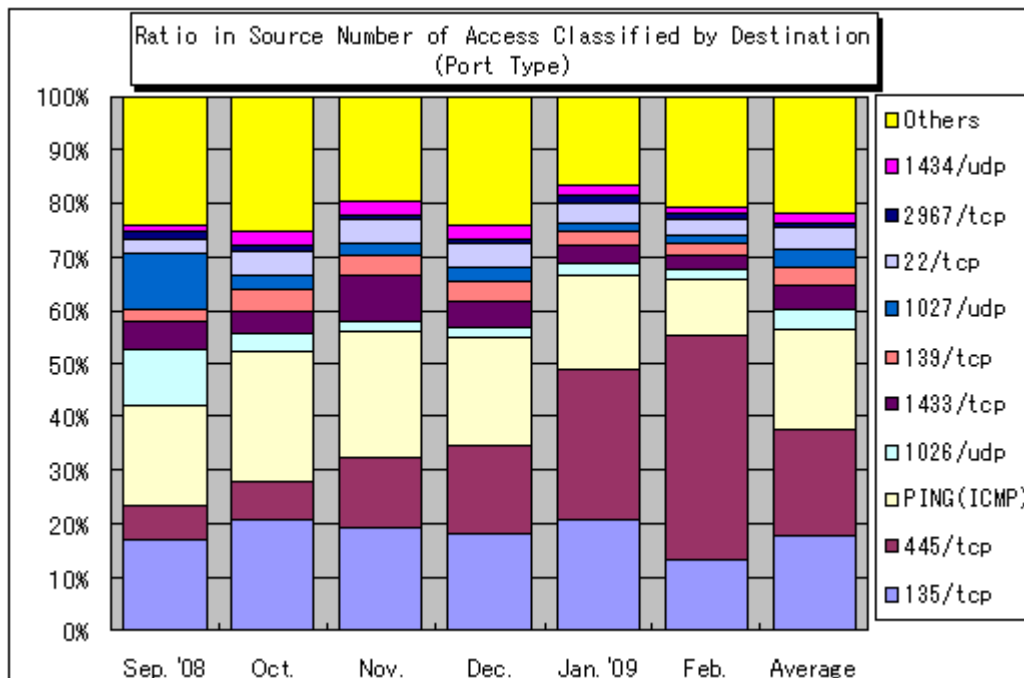
**IV. Statistic Information**

**(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 February 2009.



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



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

(3) 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 September 2008 to February 2009.

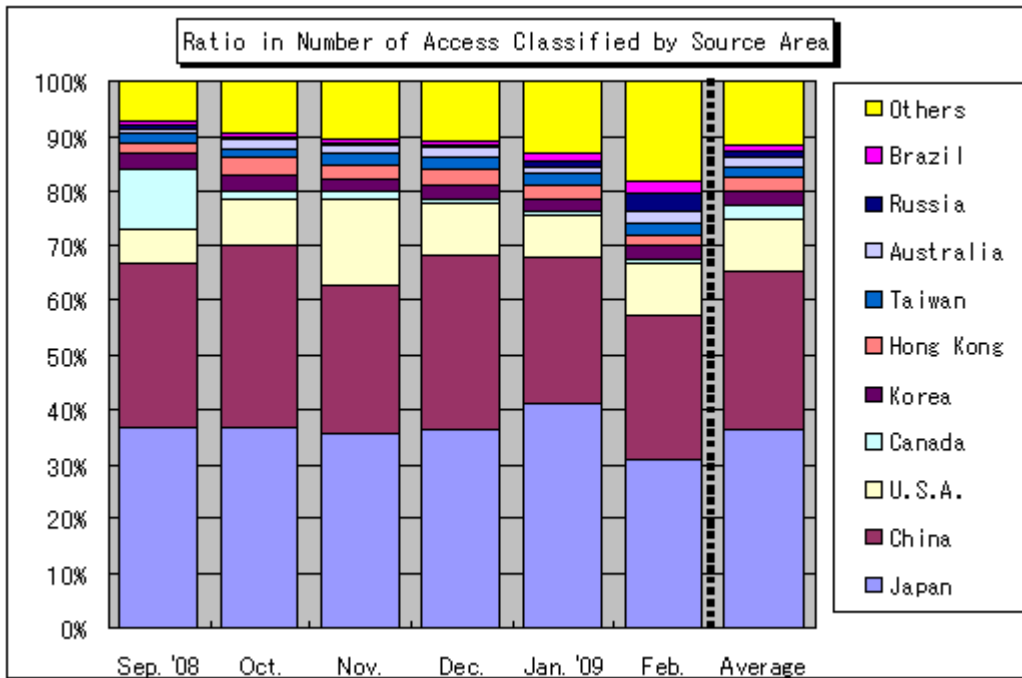


Chart 4-3: Ratio in Number of Access Classified by Source Area from September 2008 to February 2009

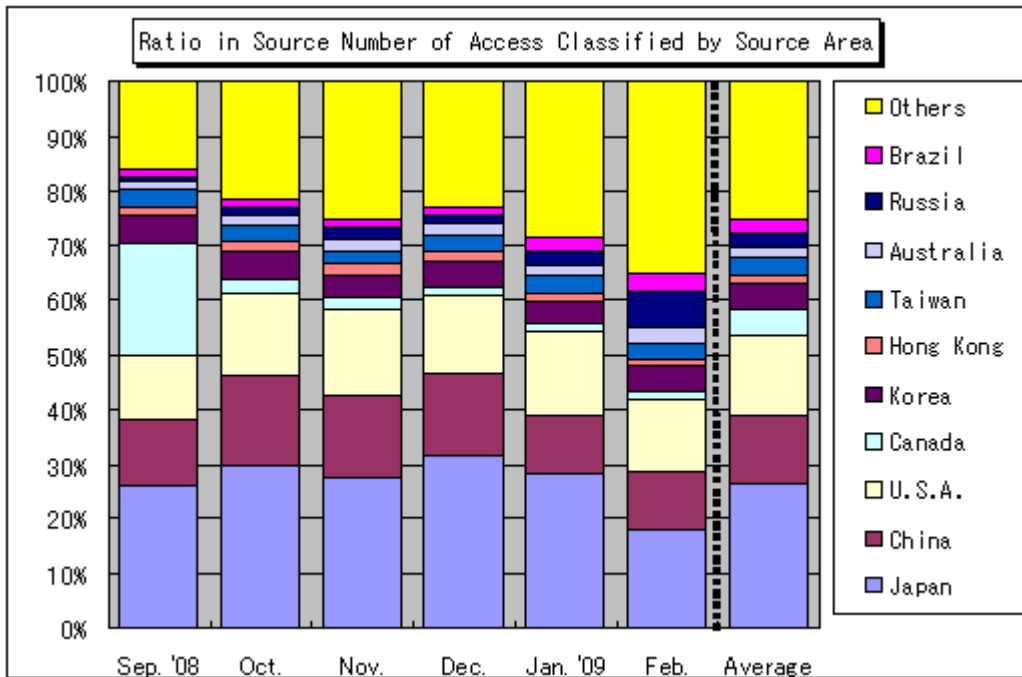


Chart 4-4: Ratio in Source Number of Access Classified by Source Area from September 2008 to February 2009

## V. 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	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.
21897/tcp	The purpose of this access has not yet clearly identified: This may be the attempts to re-connect to the IP address allocated to a file sharing software previously.

***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)