Internet Infrastructure Review

IIJ
Internet Initiative Japan

Vol.4

August
2009

Infrastructure Security

Diversification of Malware Infections

Broadband Traffic

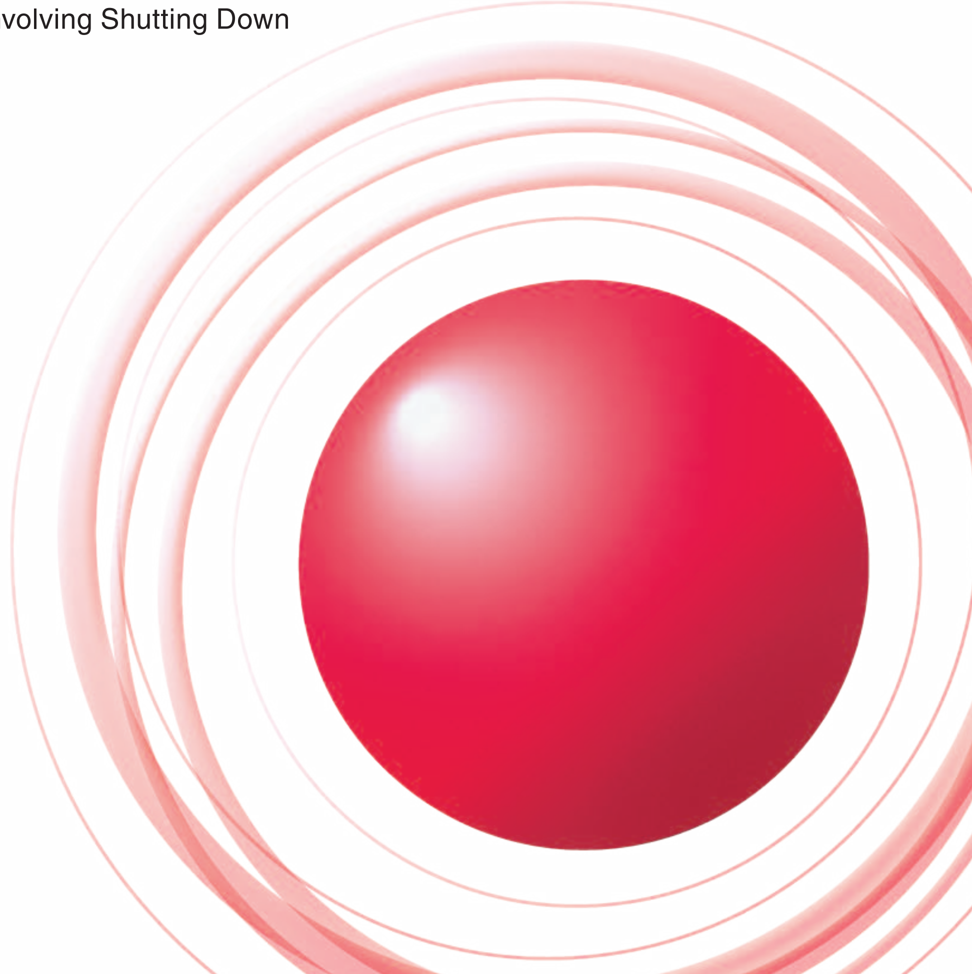
Increasing Traffic for General Users

Cloud Computing Technology

Implementation and Application of the DDD Distributed System

Messaging Technology

Limitations of Anti-Spam Measures Involving Shutting Down
the Control Source of Botnets



Internet Infrastructure Review Vol.4 August 2009

■ To download the latest issue of the Internet Infrastructure Review, please visit (http://www.iij.ad.jp/en/development/iir/).

Executive Summary

Information and Communications in Japan 2009, an annual white paper published by the Ministry of Internal Affairs and Communications on July 10, begins with a special feature titled "Why Information and Communications are Necessary for Recovery in Japan." This whitepaper points out the contributions that information and communications can make to the growth of the economy and society, while finding that although Japan has a world-class information and communications infrastructure, it is lagging behind in its utilization, with information and communications not being linked to economic strength. Furthermore, it presents the opinion that we can accelerate recovery from the economic crisis by promoting the utilization of our information and communications infrastructure, and addressing concerns about its use in both the private sector and the public sector, including government and local public bodies.

This is the fourth IIJ technical whitepaper that we have published. In Vol.4 we summarize the status of utilization and security, seen as the key to economic development in the previously mentioned whitepaper. We have approached this from the perspective of a company responsible for Internet technology infrastructure, focusing on statistical information from April 1 to June 30, 2009.

First of all, in “Broadband Traffic” we address utilization by analyzing the traffic conditions in our world-class broadband environment. The results show that due to active use of rich content such as video the average daily download usage levels for general users after excluding heavy users of P2P file sharing applications have skyrocketed a staggering 356% from 32 MB to 114 MB when compared to data from five years ago.

On the security front, in “Infrastructure Security” we comment on the Conficker malware for which large-scale infections continue, and Gumblar, which infects PCs simply through the viewing of Web content and steals information, in addition to demonstrating sophisticated behavior such as mutation and the destruction of evidence. In “Messaging Technology” we continue on from Vol.3 and explain the current status of sender authentication technologies and the importance of sender side countermeasures for the reduction of spam.

In this volume we also take on the topic of cloud computing, which is gaining a lot of attention in the field of infrastructure technology. Foreign corporations such as Google, Amazon, and Microsoft have taken the lead in this field, but evaluation of its applications in both the public and private sectors has also begun in Japan, and IIJ is proceeding with technical development in order to hopefully play a key role in its adoption here. In “Cloud Computing Technology”, we introduce IIJ's initiatives towards constructing a distributed file system that will serve as infrastructure for a cloud environment, and in “Infrastructure Security” we discuss the topic of security for cloud computing.

It goes without saying that in order to utilize information and communications effectively, security for ensuring safe use is essential. There were reports that in July government agencies and key Websites in the United States and South Korea were targeted in large-scale DDoS (Distributed Denial of Service) attacks, causing some sites to become inaccessible, and significantly affecting social activities. To prevent incidents such as this, and operate information and communications infrastructure as a stable social infrastructure, it is crucial for organizations engaged in the administration of information and communications infrastructure to respond in a coordinated manner, using the sharing of perceptions on actual conditions such as those detailed in this IIR as a starting point.

IIJ actively adopts new technologies while providing Internet infrastructure with a focus on stability and safety, and will continue its cooperative initiatives with information transmitters and related organizations, striving to further enhance the benefits of the Internet as an infrastructure for enriching society.

Author:
Junichi Shimagami
Director of IIJ, and Division Director of the Network Service Department. Mr. Shimagami has been involved in the construction and operation of infrastructure for IIJ’s backbone network, and the A-Bone international Internet backbone network that connects each country in the Asia Pacific region. In addition to backbone operation, he also currently supervises IIJ’s ISP services, such as Internet access, email, and www application outsourcing.

1 Infrastructure Security

1.1 Introduction

This whitepaper summarizes incidents to which IIJ responded, based on general information obtained by IIJ itself related to the stable operation of the Internet, information from observations of incidents, information acquired through our services, and information obtained from companies and organizations that IIJ has cooperative relationships with.

This volume (Vol.4) covers the period of time from April 1 through June 30, 2009. A number of incidents occurred during this period; we will be addressing the most representative of those in this whitepaper.

Infections of Conficker variants were repeatedly reported during the period in question (Conficker first came to prominence last year). There was also a flare-up of malware that steals information such as IDs and passwords, with infections caused by merely viewing Web content that had been altered.

Several vulnerabilities were discovered in browser plug-in software such as Adobe Reader and Apple QuickTime, and there have been reports of exploitation of these vulnerabilities.

Outside Japan, there were a number of incidents that affected large numbers of users, such as an attack on DNS servers in China, and DDoS attacks related to the presidential election in Iran.

IIJ observed that Internet-based malware activities, DDoS attacks, and SQL injection attacks on Web servers continue at about the same pace as the past periods.

As seen above, the Internet continues to experience many security-related incidents.

1.2 Incident Summary

Here, we discuss the IIJ handling and response to incidents that occurred between April 1 and June 30, 2009. Figure 1 shows the distribution of incidents handled during this period, while Table 1 provides an explanation of categorizations.

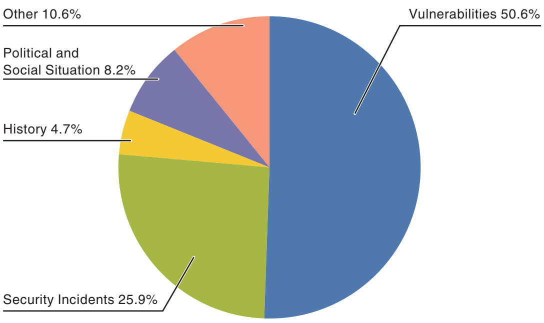


Figure 1: Incident Ratio by Category (April 1 to June 30, 2009)

Table 1: Incident Categories

Category Name	Explanation
Vulnerabilities	Indicate responses to vulnerabilities associated with network equipment, server equipment or software used over the Internet, or used commonly in user environments. Vulnerabilities, information about attacks on vulnerabilities, information from vendors regarding response to vulnerabilities, response steps taken, etc.
Political and Social Situation	Indicates responses to incidents related to domestic and foreign circumstances and international events. Responses to international conferences attended by VIPs, attacks originating in international disputes; measures taken in response to warnings/alarms, detection of incidents, and so forth.
History	Historically significant dates; warning/alarms, detection of incidents, measures taken in response, etc., related to an attack in connection with a past historical fact.
Security Incidents	Unexpected incidents and related response. Wide propagation of network worms and other malware; DDoS attacks against certain websites. Include response to incidents for which the cause was not clearly determined.
Other	Incidents not otherwise categorized. Includes those incidents not directly associated with security problems, including highly concentrated traffic associated with a notable event.

■Vulnerabilities

During this period, vulnerabilities were discovered in user applications such as WordPad and Office Text Converters*1, and Microsoft Office PowerPoint*2. Many vulnerabilities were also discovered in applications launched through Web browsers, including multiple vulnerabilities in Adobe Acrobat, Adobe Reader*3*4, and Apple QuickTime*5. These were exploited along with vulnerabilities in Flash Player*6 that were discovered earlier. Multiple vulnerabilities were also discovered in the VMware*7 virtualization software.

■Political and Social Situation

IIJ pays close attention to various political and social situations related to international affairs and current events. For this period, we focused in particular on developments related to the North Korean missile launch, the worldwide outbreak of a new strain of influenza, and the presidential election in Iran. With regard to the new strain of influenza, there were incidents of email sent with malware attachments disguised as alerts around the time that infections began occurring in Japan*8.

In Iran, there were reports of DDoS attacks*9 stemming from dissatisfaction with the results of the presidential election there. Additionally, we were on alert during the visit of national guests to Japan in May and June, but no related attacks were detected.

■History

The period in question included several historically significant days on which incidents such as DDoS attacks and Website alterations have occurred. However, IIJ did not detect any related attacks on IIJ facilities or client networks.

■Security Incidents

The largest of unanticipated incidents was the spread of Conficker variants. See “1.4.1 Worldwide Outbreak of the Conficker Malware.”

There were also a large number of reported infections of the Gumblar malware, which spreads through the viewing of altered Web content, and steals IDs and passwords. See “1.4.2 ID/Password Stealing Gumblar Malware.”

*1 Microsoft Security Bulletin MS09-010, Vulnerabilities in WordPad and Office Text Converters Could Allow Remote Code Execution (http://www.microsoft.com/technet/security/Bulletin/MS09-010.mspx).

*2 Microsoft Security Bulletin MS09-017, Vulnerabilities in Microsoft Office PowerPoint Could Allow Remote Code Execution (http://www.microsoft.com/technet/security/Bulletin/MS09-017.mspx).

*3 May 2009 Adobe - Security bulletins APSB09-06 Security Updates available for Adobe Reader and Acrobat (http://www.adobe.com/support/security/bulletins/ apsb09-06.html).

*4 Jun 2009 Adobe - Security bulletins APSB09-07 Security Updates available for Adobe Reader and Acrobat (http://www.adobe.com/support/security/bulletins/apsb09-07.html).

*5 About the security content of QuickTime 7.6.2 (http://support.apple.com/kb/HT3591?viewlocale=en_US).

*6 Feb 2009 APSA09-01 Flash Player update available to address security vulnerabilities (http://www.adobe.com/support/security/bulletins/apsb09-01.html).

*7 VMware Security Advisories (VMSAs) VMSA-2009-0006(http://www.vmware.com/security/advisories/VMSA-2009-0006.html).

*8 Beware of emails regarding Swine Flu claiming to be from the National Institute of Infectious Diseases (http://www.nih.go.jp/niid/misc/warning090428.html). (in Japanese)

*9 Information related to the attacks can be found on sites such as the following blog. THE ARBOR NETWORKS SECURITY BLOG, Iran DDoS Activity: Chatter, Tools and Traffic Rates (http://asert.arbornetworks.com/2009/06/iran-ddos-activity-chatter-tools-and-traffic-rates/).

In April, there were multiple attacks that overloaded DNS cache servers by issuing large quantities of DNS queries that return large responses*[10]. In May, a DDoS attack on DNS servers in China caused extensive connection failures for several hours*[11]. Additionally, a DoS attack tool*[12] that affects several HTTP servers was released, and information suggests it was used in DDoS attacks in Iran*[13].

■Other

As far as incidents not directly related to security, a routing information failure affecting Google drew attention when it caused a worldwide reduction in traffic*[14]. We also intermittently observe SIP communications that may cause silent phone calls to be received over IP telephony.

1.3 Incident Survey

Of those incidents occurring on the Internet, IIJ focuses on those types of incidents that have infrastructure-wide effects, continually conducting research and engaging in countermeasures. In this section, we provide a summary of our survey and analysis results related to the circumstances of DDoS attacks, malware infections over networks, and SQL injections on Web servers.

1.3.1 DDoS Attacks

Today, DDoS attacks on corporate servers are almost a daily occurrence. The methods involved in DDoS attacks vary widely. Generally, however, these attacks are not the type that utilize advanced knowledge of such as vulnerabilities, but rather cause large volumes of unnecessary traffic to overwhelm network bandwidth or server processes for the purpose of hindering services.

*10 See discussions such as the thread starting from the following post on the DNS OARC site for more information on these DNS cache server attacks (https://lists.dns-oarc.net/pipermail/dns-operations/2009-April/003779.html).

*11 Reports such as the following contain more information regarding this incident. Network World, Inc., DNS attack downs Internet in parts of China (http://www.networkworld.com/news/2009/052109-dns-attack-downs-internet-in.html).

*12 This technique overloads a Web server by sending a partial HTTP request to the server, maintaining a connection while not allowing the request to be completed. Technical details can be found at the following blog. CERT/CC Vulnerability Analysis Blog: Mitigating Slowloris (http://www.cert.org/blogs/vuls/2009/07/slowloris_vs_your_webserver.html). Also refer to information regarding measures to take for the Web server you are using, as whether or not it will be affected by this problem, and the corresponding countermeasures differ depending on the implementation.

*13 For example, on SANS ISC, Handler's Diary: Slowloris and Iranian DDoS attacks (http://isc.sans.org/diary.html?storyid=6622).

*14 See THE ARBOR NETWORKS SECURITY BLOG: The Great GoogleLapse (http://asert.arbornetworks.com/2009/05/the-great-googlelapse/) for more information on the effects of this incident on communications. There are reports that traffic for Google was redirected to Asia (Japan), but the details are not known. IIJ observed no routing or traffic anomalies during this time period.

Figure 2 shows the circumstances of DDoS attacks handled by the IIJ DDoS Defense Service between April 1 and June 30, 2009.

This information shows traffic anomalies judged to be attacks based on IIJ DDoS Defense Service standards. IIJ also responds to other DDoS attacks, but these incidents are excluded from the figure due to the difficulty in accurately ascertaining the facts of each situation.

There are many methods that can be used to carry out a DDoS attack. In addition, the capacity of the environment attacked (bandwidth and server performance) will largely determine the degree of the effect. The statistics in Figure 2 categorize DDoS attacks into three types: attacks on bandwidth capacity*[15], attacks on servers*[16], and compound attacks (several types of attacks on a single target conducted at the same time).

During the three months under study, IIJ dealt with 114 DDoS attacks. This averages to 1.25 attacks per day, but represents a decline in average incidents compared to our prior whitepaper. Bandwidth capacity attacks accounted for 1% of all incidents. Server attacks accounted for 86% of all incidents, and compound attacks accounted for the remaining 13%. The largest SYN flood was approximately 67,000pps, and the largest bandwidth attack traffic volume was around 125Mbps. During this period, an ICMP flood of more than 150,000pps was observed, but as each packet was small, the impact on bandwidth capacity was only approximately 77Mbps. Of all attacks, 83% ended within 30 minutes of commencement, while the remaining 17% lasted anywhere from 30 minutes to up to 24 hours. During the time period under study, IIJ did not note any attacks that exceeded 24 hours in length.

In most cases we observed an extremely large number of IP addresses, whether domestic or foreign. We believe this is accounted for by the use of IP spoofing*[17] and botnet*[18] usage.

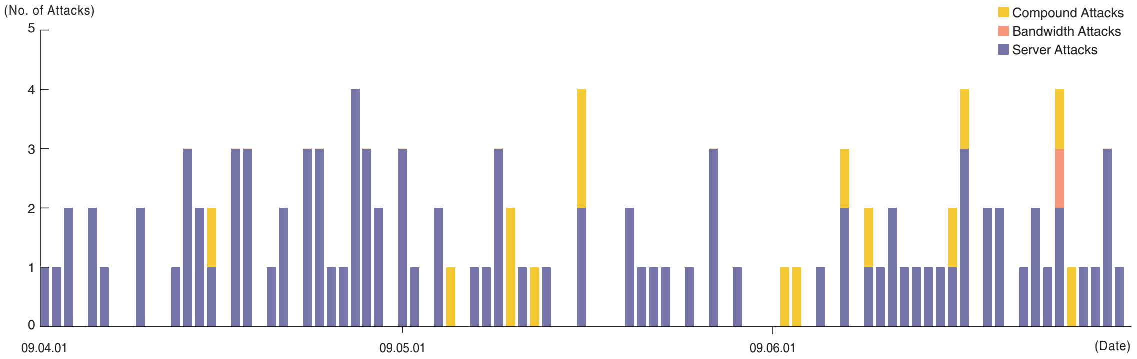


Figure 2: DDoS Attacks

*15 Attack that overwhelms the network bandwidth capacity of a target by sending massive volumes of larger-than-necessary IP packets and fragments. The use of UDP packets is called a UDP flood, while the use of ICMP packets is called an ICMP flood.

*16 TCP SYN flood, TCP connection flood, and HTTP GET flood attacks. TCP SYN flood attacks send mass volumes of SYN packets that signal the start of TCP connections, forcing the target to prepare for major incoming connections, causing the wastage of processing capacity and memory. TCP Connection flood attacks establish mass volumes of actual TCP connections. HTTP GET flood attacks establish TCP connections on a Web server, and then send mass volumes of HTTP GET protocol commands, wasting processing capacity and memory.

*17 Misrepresentation of a sender's IP address. Creates and sends an attack packet that has been given an address other than the actual IP address of the attacker in order to pretend that the attack is coming from a different location, or from a large number of individuals.

*18 A "bot" is a type of malware that institutes an attack after receiving a command from an external C&C server. A network constructed of a large number of bots acting in concert is called a "botnet."

1.3.2 Malware Activities

Here, we will discuss the results of the observations of the Malware Investigation Task Force (MITF)*19, malware activity observation project operated by IIJ. The MITF uses honeypots*20, connected to the Internet in a manner similar to general users in order to observe communications arriving over the Internet. Most appear to be communications by malware selecting a target at random, or scans attempting to locate a target for attack.

■Status of Random Communications

Figure 3 shows trends in the total volumes of communications coming into the honeypots (incoming packets) between April 1 and June 30, 2009. Figure 4 shows the distribution of sender's IP addresses by country. We have taken the average per honeypot, showing the trends for incoming packet types (top ten) over the entire period subject to study.

During this period, a large amount of client-targeted scanning behavior was observed, such as communications utilized by Microsoft operating systems, 6881/UDP used by P2P file sharing software, 4899/TCP used by PC remote administration tools*21, and 2967/TCP used by Symantec client software. At the same time, communications for which the goal was not clearly identifiable, such as 10044/UDP, were also observed. Attacks on 445/TCP, etc., targeting the MS08-067*22 vulnerability, have continued since last October.

Looking at the overall sender distribution by country, we see that attacks sourced to China and Japan, 29.2% and 20.3%, respectively, were comparatively higher than the rest.

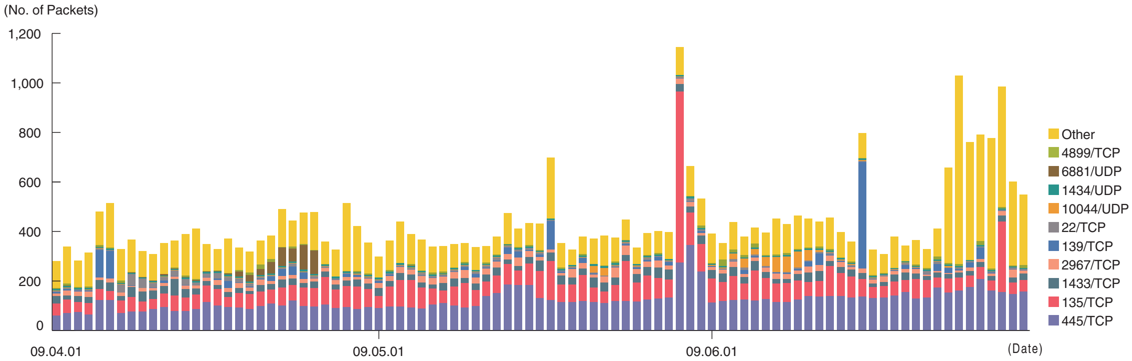


Figure 3: Communications Arriving at Honeypots (By Date, By Target Port, Per Honeypot)

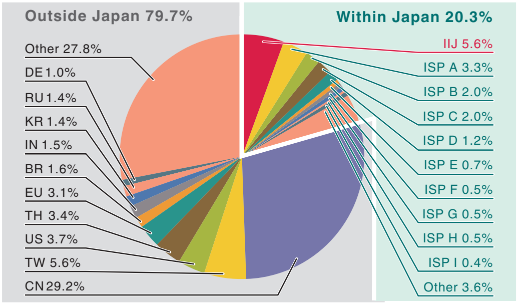


Figure 4: Sender Distribution (Entire Period under Study)

*19 Malware Investigation Task Force (MITF). The MITF began activities in May 2007 observing malware network activity through the use of honeypots in an attempt to understand the state of malware activities, to gather technical information for countermeasures, and to link these findings to actual countermeasures.

*20 A system designed to simulate damages from attacks by emulating vulnerabilities, recording the behavior of attackers, and the activities of malware.

*21 Similar scanning behavior was also observed by other organizations during the same period. For example, on SANS ISC, Handler's Diary: TCP scanning increase for 4899 (http://isc.sans.org/diary.html?storyid=6637).

*22 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).

■Malware Network Activity

Next, we will take a look into the malware activity observed by the MITF. Figure 5 shows trends in the total number of malware specimens acquired during the period under study. Figure 6 shows the distribution of the specimen acquisition source for malware. The trends in the number of acquired specimens show the total number of specimens acquired per day*[23], while the number of unique specimens is the number of specimen variants categorized according to their digest of a hash function*[24].

A total of 708 specimens were acquired per day on average during the period under study, representing about 60 different malware variants. According to last statistics, the average daily total for acquired specimens was 899, with 44 different variants. Though we see a decline in the number of specimens acquired, the number of variants remained basically unchanged.

The distribution of specimens according to source country has Japan at 56.8%, with other countries accounting for the 43.2% balance. Of the total, malware infection activity among IIJ users was 16.8%. This shows that malware infection activity continues to be localized.

The MITF prepares analytical environments for malware, conducting its own independent analyses of acquired specimens. The results of these analyses show that, during the period under observation, 5% of the malware specimens were worms, 59% were bots, and 36% were downloaders. In addition, the MITF confirmed the presence of 81 botnet C&C servers*[25] and 528 malware distribution sites.

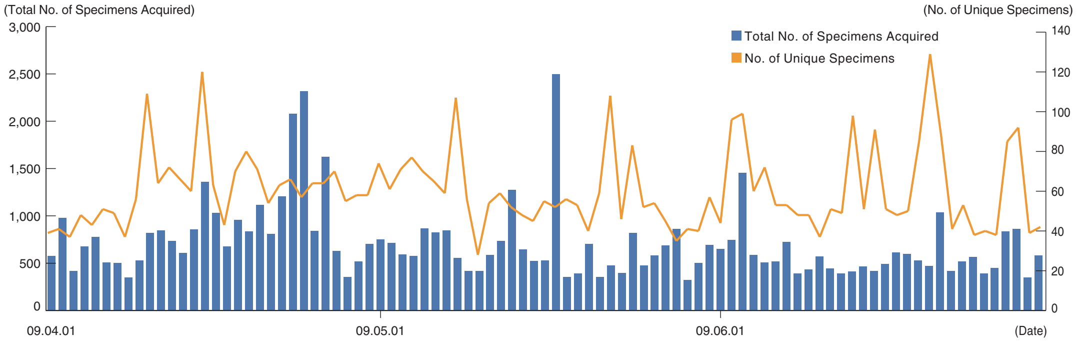


Figure 5: Trends in Number of Malware Specimens Acquired (Total Number, Number of Unique Specimens)

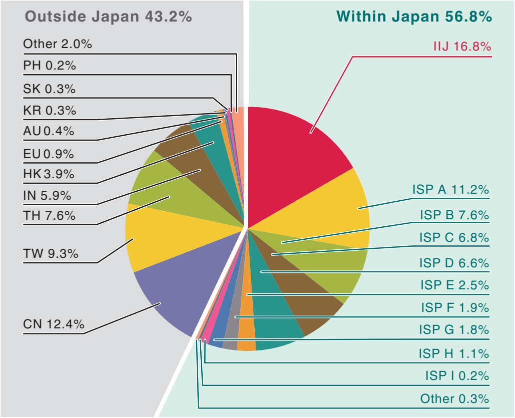


Figure 6: Distribution of Acquired Specimens by Source (Entire Period under Study)

[23] This indicates the malware acquired by honeypots.

[24] Figure derived by utilizing a one-way function (hash function) that outputs a fixed-length value for various input. The hash function is designed to produce as many different outputs as possible for different inputs. While we cannot guarantee the uniqueness of specimens by hash value, given that obfuscation and padding may result in specimens of the same malware having different hash values, the MITF has expended its best efforts to take this fact into consideration when using this methodology as a measurement index.

[25] Abbreviation for Command and Control Server. A server that sends commands to botnets comprised of numerous bots.

1.3.3 SQL Injection Attacks

Of the types of different Web server attacks, IIJ conducts ongoing surveys related to SQL injection attacks*[26]. SQL injection attacks have flared up in frequency numerous times in the past, remaining one of the major topics in the Internet security. SQL injections are known to occur in one of three attack patterns: those that attempt to steal data, those that attempt to overload database servers, and those that attempt to rewrite Web content.

Figure 7 shows trends of the numbers of SQL injection attacks against Web servers detected between April 1 and June 30, 2009. Figure 8 shows the distribution of attacks according to source. This data is a summary of attacks detected by signatures on the IIJ Managed IPS Service. The status of SQL injection attacks on Web servers is constant at the same level as our last whitepaper. The large quantity of detections on April 3 was attacks targeting a specific Web server, and as the sources of the attacks were a large number of South American IP addresses, with the same number of attacks observed from each source, we believe that this attack used a botnet. The large quantity of attacks on June 7 was from a specific address in China, and was directed at a specific Web server. Japan accounted for the source of 39.4% attacks, while China and the United States represented 34.4% and 4.9%, respectively, with other countries accounting for the rest.

The attacks above were properly detected and dealt with by the service. However, attack attempts continue, requiring ongoing attention.

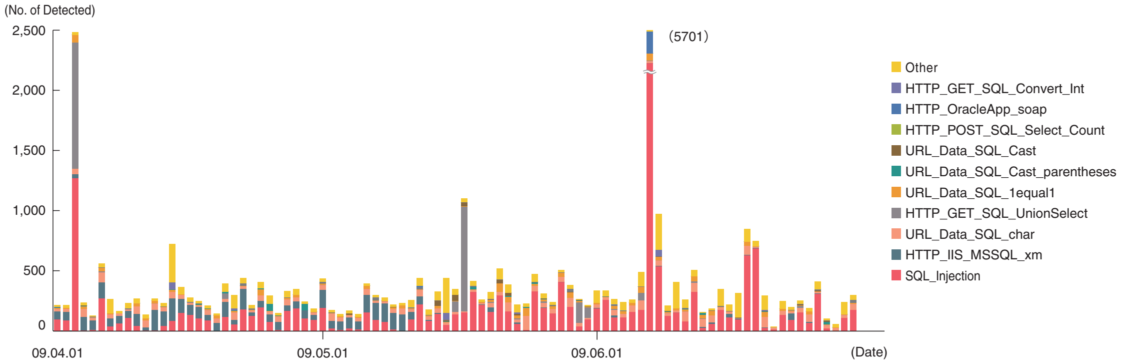


Figure 7: Trends of SQL Injection Attacks (By Day, By Attack Type)

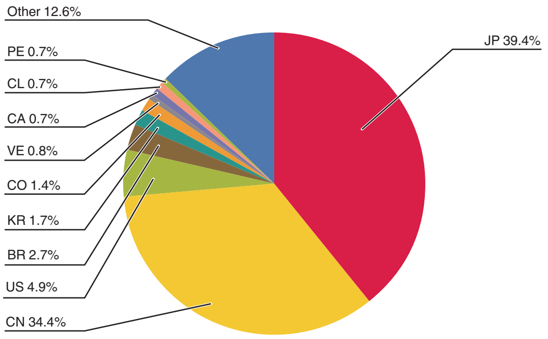


Figure 8: Distribution of SQL Injection Attacks by Source

*[26] Attacks accessing a Web server to send SQL commands, thereby manipulating an underlying database. Attackers access or alter the database content without proper authorization, and steal sensitive information or rewrite Web content.

1.4 Focused Research

Incidents occurring over the Internet change in type and scope almost from one minute to the next. Accordingly, IIJ works toward taking countermeasures by performing independent surveys and analyses. Here we will present information from the surveys we have undertaken during this period regarding the worldwide outbreak of the Conficker malware, the Gumblar malware that steals IDs and passwords, and cloud computing and security.

1.4.1 Worldwide Outbreak of the Conficker Malware

■About Conficker

Conficker is a malware that began spreading from November, 2008. Infections continue to spread due to the appearance of numerous variants, and it has gained significant attention, such as a mention in the remarks of the President of the United States in May*[27]. Here, we will discuss Conficker and the spread of Conficker infections.

■Conficker Variants and Their Behavior

Table 2 shows confirmed Conficker variants and their characteristics at the time of writing*[28]. We will describe each of their functions below.

■ Infection Activity

Conficker first exploits the vulnerability detailed in MS08-067 to infect computers over a network. It also exploits the AutoRun feature of removable media such as USB memory to infect PCs on a network protected by firewalls. Additionally, it attempts a dictionary attack*[29] on authentication information for the ADMIN$ share, and if successful it propagates across the internal network via Windows file sharing.

■ Control and Updates

Conficker updates using HTTP. The domain part of the Web server URL used for updates is determined through multiple strings (between 250 and 50,000 per day) generated using an algorithm based on the time. Individuals who attempt to control infected PCs know in advance the URLs that infected PCs will try to access on a specific day according to the algorithm, and by acquiring these domains they can control the PCs.

Table 2: Conficker Variants

Name	Date Discovered	Characteristics
Conficker.A	11/21/2008	●Exploits the vulnerability detailed in MS08-067 to infect PCs. ●Generates and accesses 250 URLs each day to attempt to update itself.
Conficker.B	12/29/2008	As Above ●Spreads by exploiting the AutoRun features of removable media such as USB memory. ●Attempts to spread via Windows file sharing.
Conficker.C (B++)	2/20/2009	As Above ●Implements a function of P2P communications, and attempts to update itself via this method.
Conficker.D (C)	3/4/2009	●As above, but generates 50,000 URLs per day, and attempts to access 500 of these. ●Changes also made to P2P communications.
Conficker.E	4/8/2009	●As above, but does not have the ability to spread via networks. ●Updated from Conficker.C or Conficker.D using P2P communications. ●Downloads other malware (such as Waledac and scareware). ●Deletes itself on May 3 (some reports indicate it was not deleted on May 3).

[27] The complete text can be viewed by following the link below. REMARKS BY THE PRESIDENT ON SECURING OUR NATION'S CYBER INFRASTRUCTURE (http://www.whitehouse.gov/the_press_office/Remarks-by-the-President-on-Securing-Our-Nations-Cyber-Infrastructure/).

[28] This table was created using information we gathered directly whenever possible, but as IIJ has not acquired all variants, missing information was based on the details published on sites such as (http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/Timeline). Conficker is also known as Downadup, and the names of its variants may also differ depending on the anti-virus software vendor or time period. For more information about this vulnerability and Conficker.A, see also IIR Vol.2 "1.4.2 Malware that Exploits MS08-067" (http://www.iij.ad.jp/development/iir/pdf/iir_vol02.pdf). (in Japanese)

[29] A dictionary attack is an attack that attempts to discover a valid password by trying each word in a pre-prepared dictionary (made up of common nouns, mechanically generated phrases, etc.).

Several variants also contain a function for updating via P2P communications. Conficker variants with this function use pure P2P communications that do not require initialization or a centralized server, and as communications are not overly concentrated, they are difficult to detect. It is believed that Conficker.E was actually propagated using this kind of P2P communications.

■ Introduction of Other Malware

Conficker.E attempts to install bots such as Waledac[*30] on PCs it has infected. If this attempt is successful, there is a possibility the PC will be taken over as part of a botnet.

■State of Infection

Conficker uses the functions detailed above to spread infections. In Japan, infections via USB memory and file sharing methods in particular have caused large-scale infections in corporate networks. A significant change in the behavior of Conficker.D on April 1 was discovered and widely reported[*31], but IIJ could not confirm any traffic anomalies on this day. Figure 9 shows the total number of incidents of Conficker.D infection activity observed by MITF[*32]. As demonstrated in this figure, almost no infection activity can be seen in Japan, but there were large quantities of such activity from China, Brazil, Europe, Russia, and the United States, in that order. According to the Conficker Working Group[*33], a total of over five million PCs have been infected[*34] with all Conficker variants at the time of writing.

As detailed above, Conficker infections are still currently being discovered in large numbers around the world, indicating that a great number of PCs could potentially be misused. This obviously poses an extremely large threat to the Internet. Because of this, many security vendors and researchers are cooperating to come up with countermeasures[*35]. As a result of limited ability of Conficker's control methods and countermeasures that have been taken, to date there have been no incidents of five million PCs being manipulated at the same time, but the situation continues to demand vigilance.

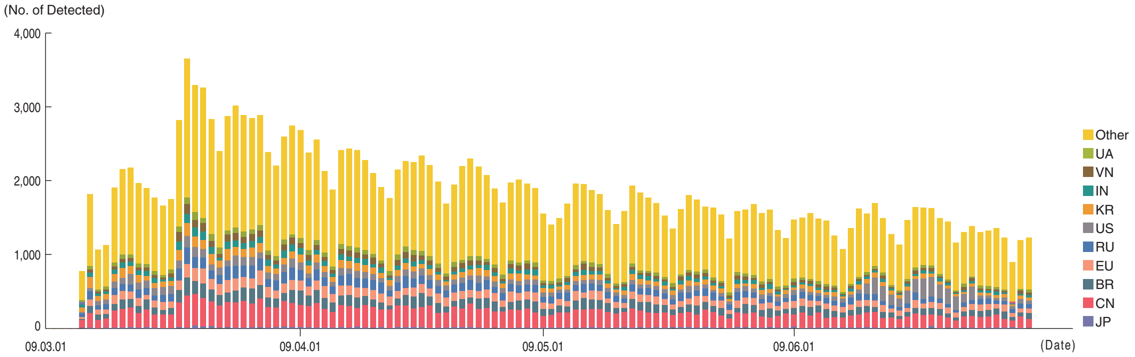


Figure 9: Conficker.D P2P Port Access (By Country)

[*30] Waledac is a form of bot that is known for sending large quantities of spam mail. See the following site for more information on the relationship between Conficker and Waledac (http://blog.trendmicro.com/downadconficker-watch-new-variant-in-the-mix/).

[*31] US-CERT technical advisory regarding Conficker. Conficker Worm Targets Microsoft Windows Systems (http://www.us-cert.gov/cas/techalerts/TA09-088A.html).

[*32] Conficker.D waits for P2P communications on ports (TCP and UDP) calculated based on the IP address of the attack target and the time. This figure is created by aggregating the sources that have accessed these P2P ports (http://nmap.org/nsedoc/scripts/p2p-conficker.html). Note that as this figure was created using observation data from all honeypots operated by IIJ including experimental ones, the population differs from that of other results such as Figure 3, and they cannot be simply compared. Additionally, Japan is placed at the bottom of the figure for ease of reference, but its actual ranking was 26th place.

[*33] The Conficker Working Group carries out activities to eradicate Conficker, and is made up of participants from many research organizations and IT vendors including security vendors. See the following URL for details on the composition of its members and activities (http://www.confickerworkinggroup.org/wiki).

[*34] Infection trends from the Conficker Working Group (http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking).

[*35] For example, because the URLs that Conficker uses to update itself are generated with an algorithm based on the date, those implementing countermeasures can also identify the URLs that Conficker will attempt to access on a specific day. This knowledge is used to monitor and respond to the actions that Conficker takes in advance.

1.4.2 ID/Password Stealing Gumblar Malware

Over the April to May period, there was a series of incidents involving stolen FTP accounts being exploited to alter Website content. The altered content then spread malware to third parties simply through them accessing it. Additionally, the malware steals personal information, IDs and passwords[*36].

■Timeline of Events

Figure 10 shows the timeline of events for this incident. The numbers in the explanation below correspond to the numbers in Figure 10.

■ From Content Alteration to Malware Infection

First, the attacker exploits a previously stolen FTP account to alter Web content (1). When a third party accesses the altered Web content (2), they are automatically redirected to a malicious Website (3) due to code such as JavaScript that was inserted when the content was altered. This script downloads a file for use in an attack to exploit vulnerabilities in applications such as Adobe Reader and Flash Player. If these vulnerabilities exist in a user's PC, the attack code in the file is executed, and malware A is downloaded (4).

■ Malware Behavior

When malware A is executed, it generates (drops) malware B, and after adding malware B to the registry it deletes itself (5). When malware B is executed, it hooks several API functions, and intercepts communications such as HTTP and FTP. It also prevents cmd.exe and regedit.exe from being executed, to make it more difficult for the infection to be detected. Additionally, it sometimes accesses other malware distribution sites, downloads new malware, and then executes it (6).

1. Using a previously stolen ID and password, the attacker alters content via FTP (inserting scripts).
2. When a user accesses an altered site, the script is executed on the Web browser.
3. Without any interaction, the user is automatically redirected to malware distribution site A.
4. Malware A is downloaded by exploiting vulnerabilities in applications such as Adobe Reader and Flash Player, and is then executed.
5. Malware A drops malware B, adds it to the registry, and then deletes itself.
6. Malware B downloads and executes new malware, intercepts FTP communications, and steals account information and uploads it to a specific server.
7. Malware B sometimes also has other behavior, such as downloading other malware, deleting traces of its activity, and deleting files on the infected PC.
8. Stolen FTP accounts are used to alter content again.
9. Stolen information is sometimes also used for fraudulent purchases and auctions.

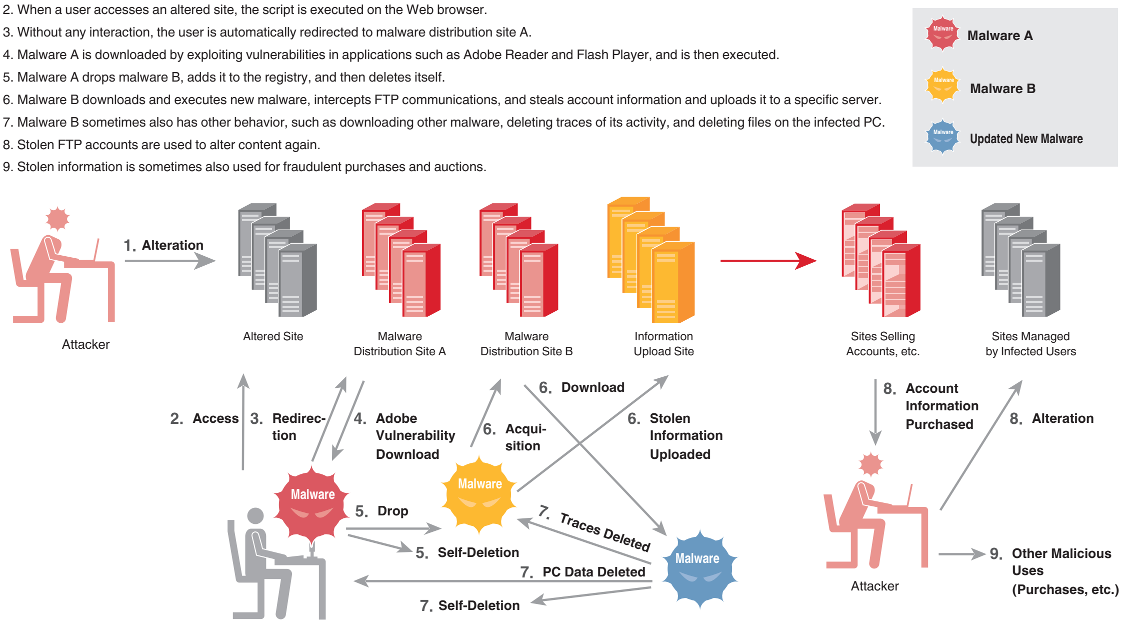

Malware A
Malware B
Updated New Malware
1. Alteration
Attacker
Altered Site
Malware Distribution Site A
Malware Distribution Site B
Information Upload Site
Sites Selling Accounts, etc.
Sites Managed by Infected Users
2. Access
3. Redirection
4. Adobe Vulnerability Download
6. Acquisition
6. Download
6. Stolen Information Uploaded
8. Account Information Purchased
8. Alteration
Malware
5. Drop
5. Self-Deletion
7. Traces Deleted
7. PC Data Deleted
7. Self-Deletion
Attacker
9. Other Malicious Uses (Purchases, etc.)

Figure 10: Anatomy of a Gumblar Incident

[*36] US-CERT Current Activity: Gumblar Malware Exploit Circulating (http://www.us-cert.gov/current/archive/2009/05/18/archive.html#gumblar_malware_attack_circulating).
Gumblar is part of the domain name of the malware distribution Website, and infections actually occurred by accessing gumblar.cn. There were similar Websites such as zlkon.lv and martuz.cn. As this incident is complicated and there is no suitable name that describes the overall situation, in this whitepaper we refer to related Websites and malware collectively as Gumblar.

■ From Upload of Information to Exploitation

Malware B, or the new, updated malware, uploads information stolen from sources such as intercepted communications and configuration files to an external server (6). This information includes personal information and ID/password details actually used during communications. The malware may also delete files which show traces of its activities, and destroy the OS or other data on the PC (7). Information stolen in this way is used to alter content once more, increasing the number of Websites that lead to new malware infections (8). As the cycle of stolen information and its misuse repeats, the situation snowballs, and it is believed that as a result a large number of users have been adversely affected. Stolen information has also caused direct financial damages through its use in identity theft and fraudulent purchases (9)*[37].

■Characteristics of Gumblar

First, as Gumblar made alterations to small-scale sites with comparatively few viewers, such as personal blogs, it took longer than usual to detect. This incident started to gain widespread attention after content was altered on a company's online shop, causing large numbers of infections.

Another of Gumblar's characteristics is the fact that it is related to multiple Websites, vulnerabilities, and other malware. In particular, the fact that the exploited malware was sequential malware*[38] made it difficult to detect, analyze, and respond to.

Additionally, the information stolen using this malware was misused only after a certain period of time had passed. Because of this, there were notable cases in which by the time the user noticed the alterations and carried out a scan using anti-virus software, the malware had already deleted itself and all traces of its activity, making it hard to detect anomalies on the PC.

At present, multiple malware distribution sites related to Gumblar have been shut down, and related malware can now be detected using anti-virus software, so it is believed the incident has been brought to a conclusion. However, we should still keep in mind that information from previously infected users still remains stolen. It is possible to construct the same circulation by simply setting up a new malware distribution site, and in fact similar incidents using other Websites and malware are still occurring on a constant basis*[39].

■Recommendations for Users

One important point for users to keep in mind regarding this issue is to pay attention to information about vulnerabilities in software installed on the PC you use, and always keep software updated to the latest version. There is a possibility that software without an automatic update function, and in particular software provided as a browser plug-in (such as Adobe Reader and Flash Player, which were exploited in this incident) will be targeted in future attacks, so make sure to update these kinds of software as well. If you discover you have become infected, you will need to change all IDs and passwords that you have entered using that computer. It is also crucial to make a habit of managing your IDs and passwords appropriately*[40].

*37 The behavior of the malware above was reproduced after analyzing specimens obtained by IIJ, but information indicates that a variety of malware other than malware A and malware B also exists, so the figure may not always be the same.

*38 Sequential malware is a system where malware is divided into separate functions, and each downloaded and executed individually when required. It is used as a method for evading anti-virus software protection. In this incident, malware such as a redirector (JavaScript malware), downloader (PDF malware, malware B), dropper (malware A), and account theft malware (malware B) were used, and they can be considered to make up one sequential malware.

*39 For example, Nine-Ball. The cNotes that indicates the alterations made by Nine-Ball can be seen on the following site (http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi?p=molo.tw). (in Japanese)

*40 See Vol.3 for more information about password management methods (http://www.iij.ad.jp/en/development/iir/pdf/iir_vol03_EN.pdf). Regarding other reference material, "Isn't Your Website being Altered," the reminder for the month from the Information-Technology Promotion Agency, Japan, contains information about countermeasures from other perspectives (http://www.ipa.go.jp/security/txt/2009/07outline.html). (in Japanese)

1.4.3 Cloud Computing and Security

Here, we will present an introduction to cloud computing, and look at security from the perspective of using cloud technology.

■About Cloud Computing

Many organizations[*41] are currently discussing the definition and standardization of cloud computing. For example, the Open Cloud Manifesto states the key characteristics of the cloud as the ability to scale and provision computing power dynamically in a cost efficient way and the ability of the consumer to make the most of that power without having to manage the underlying complexity of the technology[*42]. Amazon, Google, and Microsoft are examples of companies providing services that use cloud technology. Amazon provides the EC2 computing environment[*43] and the S3 storage service[*44] that enable users to combine, construct and operate services freely[*45]. Google is focused on providing application services such as Gmail[*46]. Microsoft provides cloud technology-based services such as Windows Live Mail (Hotmail) and Windows Update. They have also announced they will release a cloud platform service called Windows Azure[*47]. In this way, cloud technology is being applied to services as diverse as computer resources, platforms, and applications. This diversity is demonstrated in the term, "XaaS" (X as a Service). When software is provided as a service, as in Google's case, it is called SaaS (Software as a Service). Hardware, infrastructure, and platforms provided as a service are called HaaS, IaaS, and PaaS respectively. The interrelation between XaaS is shown in Figure 11.

Clouds can be classified as either public clouds or private clouds. In a public cloud, an unspecified large number of users share resources in an environment generally provided over the Internet. On the other hand, private clouds use cloud technology for limited uses rather than unspecified, large scale ones.

As detailed above, cloud computing is a form of providing resources or services. Components that make a cloud environment possible are utility computing, SOA, Web 2.0, virtualization, and the abundance of resources[*48] that can now be obtained at lower costs than ever before. These can be thought of as the technological components of the cloud. On the surface, the cloud appears to be simply a change in usage, but it incorporates other technological aspects that should be considered, such as the increasing complexity of managing vast resources and the tremendous increase in the volume of information used for management.

■Security Issues for Cloud Computing

Here we will introduce a number of points that should be considered after looking into the technological components used in cloud computing that differ from existing components.

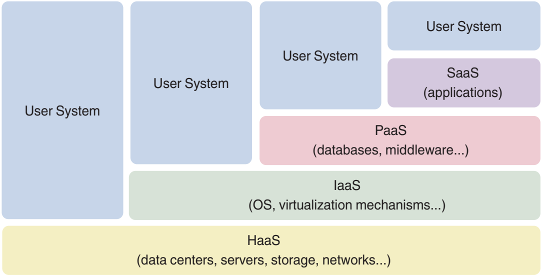

User System
User System
User System
User System
SaaS
(applications)
PaaS
(databases, middleware...)
IaaS
(OS, virtualization mechanisms...)
HaaS
(data centers, servers, storage, networks...)

Figure 11: Layers of XaaS

[*41] The organizations promoting the standardization of cloud technology include: Open Cloud Manifesto (http://www.opencloudmanifesto.org/), Open Cloud Consortium (http://www.opencloudconsortium.org/), Cloud Security Alliance (http://www.cloudsecurityalliance.org/), Open Cloud Standards Incubator (http://www.dmtf.org/about/cloud-incubator).

[*42] The source text can be found at Open Cloud Manifesto (http://www.opencloudmanifesto.org/Open%20Cloud%20Manifesto.pdf). However, this is not a definition of the cloud, but preparations for the purpose of discussion.

[*43] Amazon EC2 is short for Elastic Compute Cloud, and is a service for providing CPU resources over the Internet (http://aws.amazon.com/ec2/).

[*44] Amazon S3 is short for Simple Storage Service, and is a service for providing disk space for use with EC2 (http://aws.amazon.com/s3/).

[*45] Examples of introduction include NASDAQ Market Replay and The New York Times' TimesMachine. Market Replay is an application that makes analysis of past market trends possible, and S3 is used for the storage of data (http://aws.amazon.com/about-aws/media-coverage/2008/07/18/nasdaqs-use-ofamazon-s3). The New York Times used EC2 for the archiving of past newspapers, and the PDF conversion of pages was completed in an extremely short period of time (http://open.blogs.nytimes.com/2007/11/01/self-service-prorated-super-computing-fun/).

[*46] Starting with the well-known Gmail e-mail service, Google also provides applications such as Google Calendar for schedule management and Google Documents office tools (http://www.google.com/apps/intl/ja/business/index.html).

[*47] Windows Azure provides computing and storage environments, and also makes it possible to construct systems freely combining services such as Windows Live (http://www.microsoft.com/azure/whatisazure.mspx).

[*48] Such as the shift to many-core CPUs, data transmission channel bandwidth, memory, and the capacity of storage such as hard disks.

■ Issues Related to Boundaries

There is a greater possibility for the adverse effects of vulnerabilities to spread further than existing environments, such as unauthorized data access occurring when logically isolated resource boundaries are evaded due to vulnerabilities in the virtualization technology itself. The question of what boundaries will be set for the cloud is another new issue to be considered. Public clouds and private clouds should not be easily interconnected. Unauthorized access being made from the public side must be prevented. In addition, there is a need to prevent the vast resources from being used as a platform for further misuse, in case of the cloud being broken into.

■ API-Related Issues

APIs are generally used to control a cloud, so the impact of vulnerabilities being discovered in those APIs must be considered. This impact will be more wide-ranging than existing environments, as it can lead to not only unauthorized use of individual services in the cloud, but also unauthorized operation (including shutdown) of the cloud itself. The countermeasures against the theft of authentication information for accessing APIs or a cloud management terminal being compromised, are similar to existing security measures. However, it is expected that the impact will be much larger for clouds.

■ Digital Forensics

Another big issue is how digital forensics*[49] will be carried out. As the cloud often separates physical entities and logical entities, the monitoring of communications, analyses of hard drive images, and the investigation of logs will become extremely difficult. It will also be necessary to obtain and store a larger quantity of administrative information that indicates the status of the components the cloud is composed of.

■Using the Cloud Safely

Using cloud technology means entrusting the cloud with the management and processing of various data. For example, it is of concern whether or not the CIA (confidentiality, integrity, availability) of data in the cloud can be managed appropriately from the user's perspective. This is also a concern we face with existing outsourcing methods, and by making appropriate situational use of the cloud, and enforcing compliance with contractual and operational rules, countermeasures identical to those already in place can be considered (Figure 12).

However, as already detailed under technological components, there are differences between existing forms of outsourcing and the cloud in the areas of increasing complication in systems based on virtualization technology and the constantly climbing volume of administrative information for resources. Conversely, if these two points can be dealt with, the same level of security as existing environments can be achieved when using cloud technology. Regarding the first issue, we are making a study*[50] of a model similar to that shown in Figure 13 for understanding the dependencies between OS and applications for systems configured using the cloud, methods for isolating and segmenting these systems, and structures for access control. As for the second issue, it will be important to create a data model of the system, and

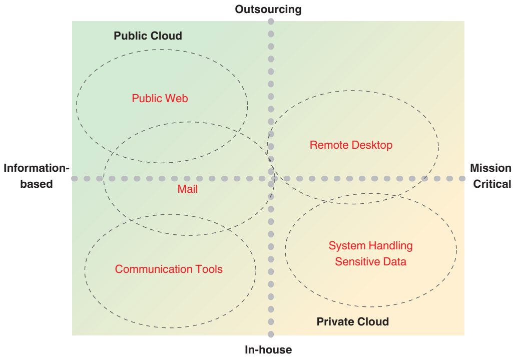


Figure 12: Proper Use of Services Based On System Purpose

*[49] NPO The Institute of Digital Forensics defines this as a series of scientific investigation methods and technology for the preservation, investigation and analysis of electromagnetic records, as well as analysis and information gathering regarding the alteration or damage of electromagnetic records, for the purpose of incident response, legal disputes, and litigation (http://www.digitalforensic.jp/wdfitm/wdf.html). (in Japanese)

*[50] A. Kanaoka, M. Kato, N. Todo, E. Okamoto: Networked System Modeling and its Access Control Characteristic Analysis, Proceedings of World Academy of Science, Engineering and Technology (WASET), Vol. 35, pp.125-133 (2008)

implement automatic computer management. By creating a model of the vast and complex structure of the cloud environment, it will be possible to automatically confirm the scope of the impact when an anomaly occurs*[51], and control the situation.

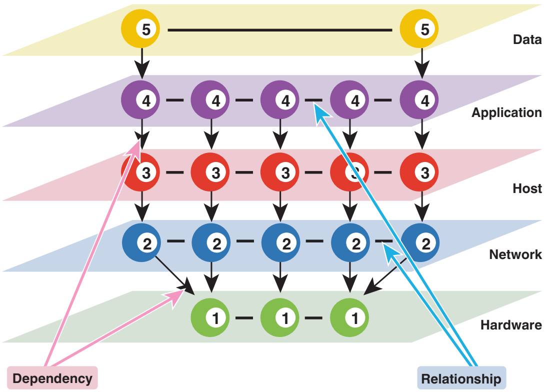
In this section, we have summarized a variety of security-related concerns with cloud computing. With the ever-advancing aggregation and optimization of information systems, opportunities to use cloud computing technology will inevitably be more frequent in the future. As indicated in this section, if consideration is given to the proper use of existing environments and cloud computing, after first understanding of the mechanisms and structure of the cloud, it will be possible to gain the unique benefits of cloud computing while maintaining a secure environment.

1.5 Conclusion

This whitepaper has provided a summary of security incidents to which IIJ has responded. In this volume (Vol. 4), in addition to detailing the current outbreak of two serious threats, we discussed security measures for cloud computing environments.

On top of responding to incidents that are causing damage here and now, it is also important to occasionally take a good look at constantly changing technological trends, and prepare for future incidents by anticipating them and considering countermeasures.

By identifying and publicizing incidents and associated responses in whitepapers such as this, IIJ will continue to inform the public about the dangers of Internet usage, providing the necessary countermeasures to allow the safe and confident usage of these important components of the social and corporate infrastructure.



The numbered balls represent resources to be managed. Each resource has attributes (device, OS, application name, etc.). The lines connecting resources on each layer indicate relationships between the resources on that layer (such as communication between applications, etc.). Lines between layers represent resource dependencies. By expressing the items to manage in the cloud in a model such as this, it is possible to confirm the scope of the impact when, for example, there is a failure in a component of the hardware.

Figure 13: Examples of Logical Expressions for Cloud-Based Systems

Authors:
Mamoru Saito
General Manager of the Division of Emergency Response and Clearinghouse for Security Information, IIJ Service Business Department
After working in security services development for enterprise customers, Mr. Saito became the representative of the IIJ Group emergency response team, IIJ-SECT in 2001, participating in FIRST, an international group of CSIRTs. Mr. Saito serves as a steering committee member of several industry groups, including Telecom-ISAC Japan, Nippon CSIRT Association, Information Security Operation provider Group Japan, and others.

Hirohide Tsuchiya (1.2 Incident Summary), **Tadaaki Nagao**, **Yuji Suga**, **Shigeki Ohara**, **Hiroshi Suzuki** (1.3 Incident Survey)
Hiroshi Suzuki, **Takeshi Umezawa** (1.4.1 Worldwide Outbreak of the Conficker Malware),
Hiroshi Suzuki (1.4.2 ID/Password Stealing Gumblar Malware)
Masahiko Kato (1.4.3 Cloud Computing and Security)
Division of Emergency Response and Clearinghouse for Security Information, IIJ Service Business Department

Contributors:
Yasunari Momoi, Service Promotion Section, Security Service Division, IIJ Network Service Department
Shigeki Ohtsu, **Yasumitsu Makino**, System Infrastructure Division, IIJ Service Business Department
Kiyotaka Doumae, Planning Section, Data Center Business Planning and Operations Division, IIJ Service Business Department

*51 M. Kato, A. Kanaoka, N. Todo, E. Okamoto: Visualization and Measurement of Vulnerability Impact on Networked System, Computer Security Symposium 2008 (CSS2008) (2008)

2 Broadband Traffic

2.1 Introduction

In this whitepaper we will analyze traffic for the broadband access services that IIJ operates, and present our findings.

It has been reported that growth in Internet traffic levels over the past five years has been comparatively stable both in Japan and internationally (see references 3, 4, and 5, p.23). The total volume of broadband traffic in Japan is increasing at an annual rate of 30%, and this represents approximately 60% of the overall backbone traffic in Japan. The majority of individual Internet users have broadband access so that identifying broadband traffic trends is also important for understanding overall traffic. (See references 1 and 2, p.23).

This whitepaper examines recent broadband traffic trends based on the daily traffic volume of users and usage levels by port. Heavy users of communication applications such as P2P file sharing still account for a dominant portion of traffic volume, but traffic attributed to these users has not increased significantly. On the other hand, the volume of traffic attributed to general users is steadily increasing, due to a surge in video content and content-rich websites.

2.2 About the Data

The survey data utilized in this whitepaper was collected using Sampled NetFlow from the routers accommodating fiber-optic and DSL broadband customers of our personal and enterprise broadband access services. Because broadband traffic trends vary between weekdays and weekends, we analyzed a full week of traffic, in this case the period from May 25 to May 31, 2009. For comparison, we used the period from February 21 to February 27, 2005. In 2005, video sharing services such as YouTube and Nico Nico Douga had yet to appear.

The usage levels of each user were obtained by matching the IP address assigned to each user with the IP addresses observed. We collected statistical information by sampling packets using NetFlow. The sampling rate was set to either 1/1024, 1/2048, 1/4096, or 1/8192, depending on router performance and load. We estimated overall usage levels by multiplying observed usage levels by the reciprocal of the sampling rate. Depending on the sampling rate, there may be slight estimation errors in data for low-volume users, but for users with reasonable usage levels we were able to obtain statistically meaningful data.

Approximately the same numbers of fiber-optic and DSL users were observed as in 2005. However, the migration to fiber-optic connections advanced in 2009, with 84% of the observed users now using fiber-optic connections, which represent 90% of the overall volume of traffic.

The IN/OUT traffic presented in this whitepaper indicates directions from an ISP's perspective, with IN representing uploads from users, and OUT representing user downloads.

2.3 Daily Usage Levels for Users

First, let us examine the daily usage levels for broadband users from several perspectives. Daily usage indicates the average daily usage for each user over the period of a week.

Figure 1 indicates the average daily usage distribution (probability density function) per user, divided into uploads (IN) and downloads (OUT), with user traffic volume on the X axis, and probability density of users on the Y axis. The X axis indicates volumes between 10^4 (10 KB) and 10^{11} (100 GB) using a logarithmic scale. Some users are outside the scope of the graph, with usage for the highest volume users climbing to over 200 GB, but most fall within the scope of 10^{11} (100 GB). A slight spike appears on the left side of the

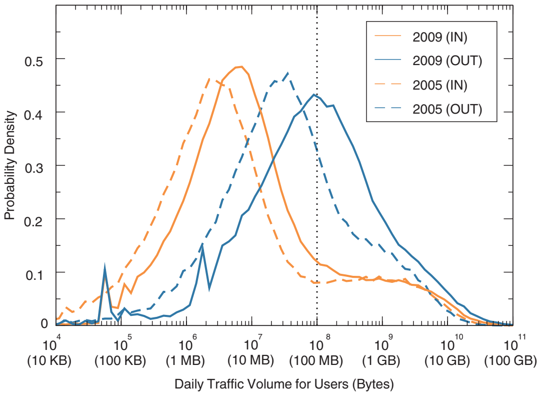


Figure 1: Daily User Traffic Volume Distribution

2009 graph, but this is just noise caused by the coarser sampling rate according to increased traffic.

The distribution for IN and OUT shows almost log-normal distribution, which is the normal distribution in a semi-log graph. A linear graph would show a long-tailed distribution, with the peak close to the left end and a slow decay towards the right. The OUT distribution slips further to the right than the IN distribution, indicating that the download volume is an order of magnitude larger than the upload volume. As average values are pulled up by the heavy users on the right side of the graph, the average IN volume was 430 MB in 2005 and rose to 556 MB in 2009. The average OUT volume was 447 MB in 2005 and rose to 971 MB in 2009.

Looking at the right end of the IN distribution, you will notice another small peak in the distribution. In fact, a similar peak can be seen on the OUT side, overlapping with the main distribution. These distributions have IN and OUT volumes at about the same position, indicating heavy users with symmetrical IN/OUT volumes. For convenience, we will call the asymmetrical IN/OUT distribution that makes up the vast majority "client-type users," and the distribution of heavy users with symmetrical IN/OUT volumes making up a minority on the right side "peer-type users."

Comparing the most frequent distribution value for client-type users in 2005 and in 2009, the IN volume rose from 3.5 MB to 6 MB, and the OUT volume rose from 32 MB to 114 MB. This demonstrates that, particularly in the case of downloads, the traffic volume for each user has increased dramatically. In contrast, there was no significant change in the most frequent distribution value for peer-type users, which approached 2 GB in both 2005 and 2009. In other words, while usage levels for general users have increased greatly, usage levels for heavy users have remained constant.

While not shown in the figure, looking into similar distributions for both fiber-optic and DSL connections, distribution points for client-type and peer-type users are about the same for a given year, but for fiber-optic connections the ratio of peer-type users is greater. This means that while there is no difference in the typical usage levels for each distribution, there is a larger ratio of heavy users in fiber-optic connections. The figure of 2 GB per day as the most frequent distribution value for peer-type users is equivalent to 185 kbps when converted to bits/second.

Figure 2 shows daily traffic volume for users in complementary cumulative distribution form. This indicates the percentage of total users with usage levels lower than the X axis value on the Y axis using a logarithmic scale, which is an effective way of examining the distribution of heavy users. The right side of the graph falls linearly, showing a long-tailed distribution close to power-law distribution. It can be stated that heavy users are distributed statistically, and are by no means a unique type of user.

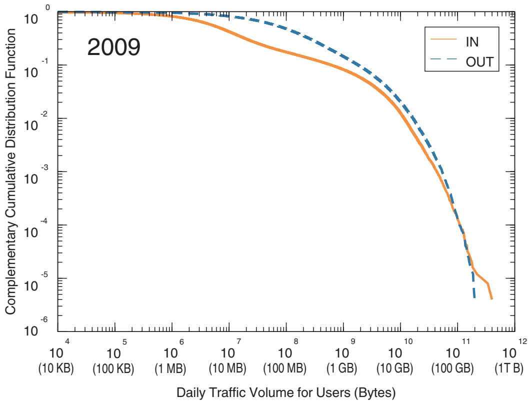


Figure 2: Complementary Cumulative Distribution of the Daily Traffic Volume for Users

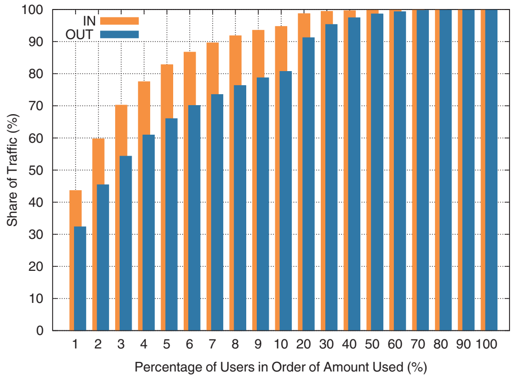


Figure 3: Traffic Usage Deviation Between Users

Figure 3 indicates the deviation in traffic usage levels between users. It shows that users with the top X% of usage levels account for Y% of the total traffic volume. There is a great deal of deviation in usage levels, and as a result traffic volume for a small portion of users accounts for the majority of the overall traffic. For example, the top 10% of users make up 80% of the total OUT traffic, and 95% of the total IN traffic. Furthermore, the top 1% of users make up 30% of the total OUT traffic, and 40% of the total IN traffic. Although minor fluctuations occur depending on the behavior of top users, this deviation is mostly unchanged from 2005. This is a characteristic of long-tailed distributions, and a trend that matches Internet data. For example, even when deviation after removing peer-type users is examined, almost the same deviation is observed. Deviations like this are not at all uncommon outside the Internet as well, and are known to appear often in large-scale, complex statistics such as the frequency of word usage and the distribution of wealth.

At a glance, you may get the impression that traffic deviations between users are polarized between those who are heavy users and those who are not. However, the distribution of usage levels follows power-law, demonstrating that a diverse range of users exist.

Figure 4 plots the individual IN/OUT usage levels for 5,000 randomly sampled users in 2005 and 2009. The X axis shows OUT (download volume) and the Y axis IN (upload volume), both using a logarithmic scale. When the IN/OUT volumes for a user are identical, they are plotted on the diagonal line.

Two clusters can be observed. The cluster below the diagonal line and spread out parallel to it is client-type general users with download volumes an order of magnitude higher than their upload volumes. The other cluster is peer-type heavy users spread out around the diagonal line in the upper right. However, the boundary between the two clusters is ambiguous. This is because client-type general users also use peer-type applications such as Skype, and peer-type heavy users also use download-based applications on the web. In other words, many users use both types of applications in varying ratios. There are also significant differences in the usage levels and IN/OUT ratio for each user, pointing to the existence of diverse forms of usage.

By comparing 2005 and 2009, we can see that the center of the client-type cluster is moving towards the upper right, and the peer-type cluster is spreading out and becoming less dense.

2.4 Usage by Port

Next, we will look at a breakdown of traffic from the perspective of usage levels by port. Recently, it has been difficult to identify applications by port number. Many P2P applications use dynamic ports on both ends, and a large number of client/server applications use port 80 assigned for HTTP to avoid firewalls. To broadly categorize, when both parties use a dynamic port higher

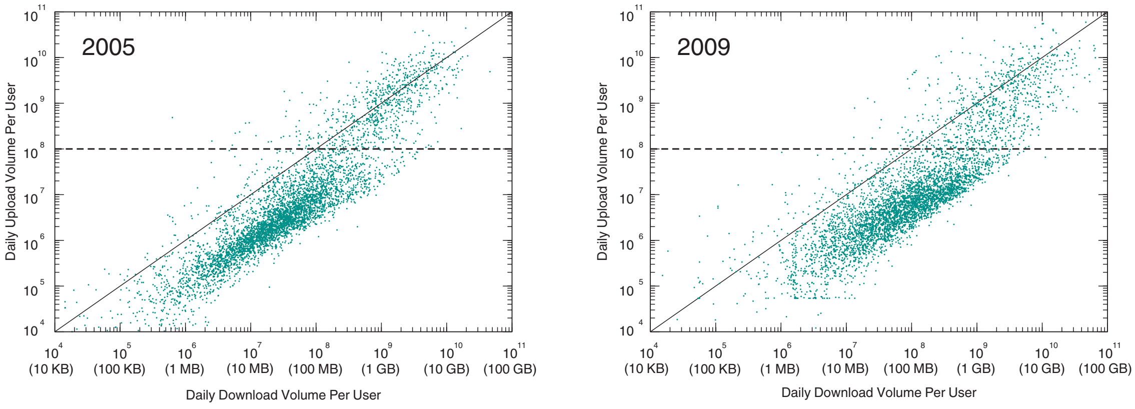


Figure 4: IN/OUT Usage for Each User, 2005 (left) and 2009 (right)

than port 1024, there is a high possibility of it being a P2P application, and when one party uses a well-known port lower than port 1024, there is a high possibility of it being a client/server application. In light of this, we will look at usage levels for TCP and UDP connections by taking the lower port number of the source and destination ports.

As overall traffic is dominated by peer-type heavy user traffic, to examine trends for client-type general users, we have taken the rough approach of extracting data for users with a daily upload volume of less than 100 MB, and treating them as client-type users. This corresponds to the intermediate point between the two IN distributions in Figure 1, and users below the horizontal line at the IN = 100 MB point in Figure 4.

Figure 5 shows an overview of port usage, comparing all users and client-type users for 2005 and 2009. Table 1 shows detailed numeric values for this figure.

Over 95% of traffic is TCP based. Looking at the overall picture, the majority of traffic is through TCP dynamic ports, with both parties using dynamic ports for 78% of the total traffic in 2009. Specific ports in the dynamic port range make up a small percentage, comprising 1.1% of the total traffic at most. Use of port 80 has increased from 9% in 2005 to 14% in 2009.

When data is limited to client-type users, port 80 is even more common, increasing from 51% in 2005 to 67% in 2009. Conversely, the ratio of dynamic ports has decreased from 36% to 18%. The second most common port was port 554. This is the port assigned to the Real-Time Streaming Protocol (RTSP), and is related to the increase in video content.

From this data, we can see that TCP traffic over port 80 is on the rise. Port 80 traffic is also used for data such as video content and software updates, so we cannot identify the type of content this is attributed to, but it demonstrates the fact that client/server communications are increasing.

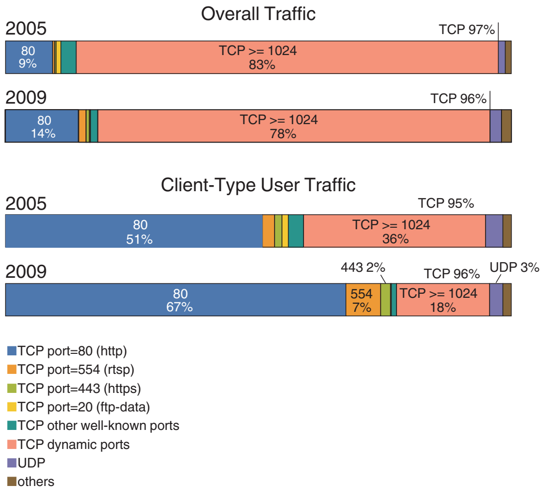


Figure 5: Usage Level Overview by Port

protocol port		2005		2009	
		total (%)	client type	total (%)	client type
TCP	*	97.43	94.93	95.80	95.73
	(<1024)	13.99	58.93	18.23	77.31
	80 (http)	9.32	50.78	14.46	67.30
	554 (rtsp)	0.38	2.44	1.48	6.89
	443 (https)	0.30	1.45	0.64	1.91
	20 (ftp-data)	0.93	1.25	0.19	0.17
	(>=1024)	83.44	36.00	77.57	18.42
	6346 (gnutella)	0.92	0.84	1.10	0.60
	6699 (winmx)	1.40	1.14	0.70	0.24
	1935 (rtmp)	0.20	0.81	0.36	1.51
	7743 (winny)	0.48	0.15	0.25	0.03
UDP	*	1.38	3.41	2.24	2.60
	53 (dns)	0.03	0.14	0.03	0.07
ESP		1.09	1.35	1.87	1.55
GRE		0.07	0.12	0.07	0.08
ICMP		0.01	0.05	0.02	0.05

Table 1: Usage Level Details by Port

Figure 6 compares trends in TCP port usage over a week for overall traffic between 2005 and 2009. This shows trends for TCP port usage divided into three categories: port 80, other well-known ports, and dynamic ports. We cannot disclose absolute amounts of traffic, so we have presented data normalized by the total peak traffic volume. Dynamic port traffic is predominant overall, with peaks between 11:00 P.M. and 1:00 A.M., and traffic increases in the daytime on Saturday and Sunday, reflecting times when the Internet is used at home.

Similarly, Figure 7 shows trends in TCP port usage over a week for client-type users. This data indicates that although port 80 usage was slightly higher than dynamic port usage in 2005, in 2009 port 80 is the predominant form of traffic. Peak times are slightly earlier, occurring between 9:00 P.M. and 11:00 P.M., and use from the morning on Saturdays and Sundays has increased.

Comparing trends for total traffic and client-type traffic, we can see that there is a difference in the drop-off in traffic after midnight. Port 80 traffic drops off suddenly after midnight, and drops to its minimum level at around 4:00 A.M. In contrast, dynamic port traffic flow slopes off gradually in the early hours of the morning, dropping to its minimum level at around 8:00 A.M. We speculate that this is influenced by files being uploaded manually in the evening and distributed overnight via P2P file sharing applications that use dynamic ports, and by users who stop applications after they have finished downloading the files that they seek.

2.5 Conclusion

As we have observed, peer-type traffic such as P2P file sharing still dominates traffic from a volume perspective, but it has not increased significantly since 2005. One possible reason for this is that users have shifted from P2P file sharing applications to services such as video sharing sites that are easier to use and more popular. This may also be influenced by the fact that P2P file sharing mechanisms have been revised not to use excessive bandwidth, as a result of the rapidly increased traffic volumes from P2P file sharing being identified as a problem. Changes in user awareness due to ISPs introducing countermeasures against excessive usage such as bandwidth cap may have also contributed.

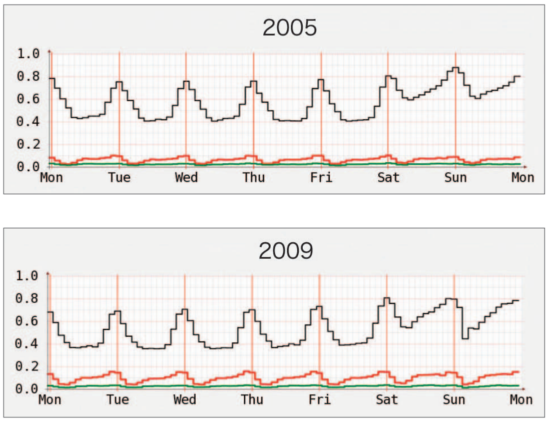


Figure 6: Weekly TCP Port Usage Trends for Overall Traffic 2005 (Top) 2009 (Bottom)

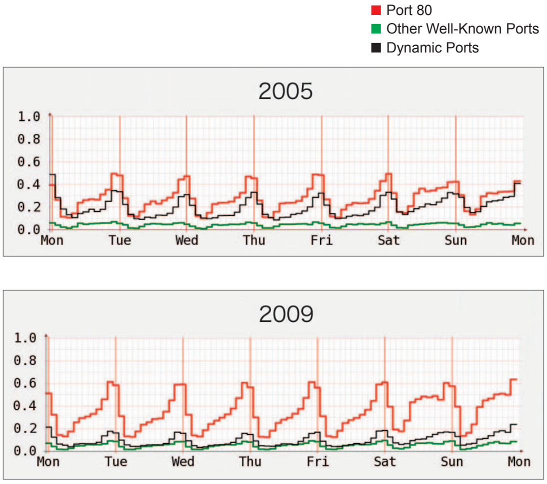


Figure 7: Weekly TCP Port Usage Trends for Client-Type Users 2005 (Top) 2009 (Bottom)

Meanwhile, usage levels for general users are steadily increasing due to rich video content and web 2.0 content. In addition to video content, there are also an increasing number of websites that automatically provide a variety of constantly changing information, or preload content in the background which a user may view next, without any explicit user action such as mouse clicks. This also leads to an increase in traffic volume.

Traffic increased dramatically around 2004 with the appearance of P2P file sharing, and this was expected to put strain on network capacity. Over the five years since then, traffic has been increasing at a stable annual rate of approximately 30%. Meanwhile, it is said that capacity for networks such as backbones has been increasing at an annual rate of approximately 50% (see reference 6). Because of this, it is believed that there is currently a surplus of bandwidth capacity on a macro level.

However, it is difficult to predict future Internet traffic based on past data. This is because the behavior of a small number of heavy users has a considerable impact, and when there is a change in this behavior, predictions can be wildly inaccurate. The way that users utilize the Internet is also influenced greatly by not only technological factors, but also by economic, social, and political ones. Additionally, just as the appearance of the web and P2P file sharing have caused an upheaval in traffic volumes, there is always the possibility of the appearance of new technology drastically changing the way the Internet is used. Considering that until now traffic volumes have undergone significant change in cycles of five or ten years, in a sense recent traffic growth has almost been too stable. Before too long we may find ourselves facing another upheaval.

IIJ monitors traffic levels on an ongoing basis so we can respond swiftly to changes in forms of Internet usage. We will continue to publish whitepapers such as this periodically.

Author:
Kenjiro Cho
Deputy Research Director, IIJ Innovation Institute Inc. Research Laboratory. Dr. Cho's research topics include the analysis of complex network dynamics in order to turn the Internet into a simpler, more flexible and more dependable communication infrastructure, QoS communications, and operating system support for networking. He is a board member of the WIDE Project, and an adjunct professor at Japan Advanced Institute of Science and Technology.

References

1: K. Cho, K. Fukuda, H. Esaki, and A. Kato.
The impact and implications of the growth in residential user-to-user traffic.
In ACM SIGCOMM2006, Pisa, Italy, Aug. 2006.

2: K. Cho, K. Fukuda, H. Esaki, and A. Kato.
Observing Slow Crustal Movement in Residential User Traffic.
In ACM CoNEXT2008, Madrid, Spain, Dec. 2008.

3: Cisco. Visual Networking Index - Forecast and Methodology, 2007-2012. June 2008.

4: Cisco. Approaching the zettabyte era. June 2008.

5: A.M. Odlyzko. Minnesota Internet traffic studies.
http://www.dtc.umn.edu/mints/home.html.

6: TeleGeography Research. Global Internet Geography. 2008.

3 Cloud Computing Technology

3.1 Introduction

It is said that cloud computing represents a paradigm shift from owning computing resources to using them. At IIJ, we have been developing and operating technology for supporting cloud computing for the past few years, in order to implement the immense data processing power and efficient infrastructure that it provides.

Here, we will explain the distributed system called "ddd," which is one of the proprietary cloud technology infrastructures that IIJ has developed and implemented, and is using as a service infrastructure.

3.2 About Distributed Systems

Before we explain ddd, we will define the distributed systems that we will discuss here. By definition, a distributed system is (1) - made up of multiple computer nodes and (2) visible as a single system to its users.

Some examples of distributed systems are distributed storage used for retaining large quantities of data, and distributed data processing. (Figure 1, Figure 2)

The purpose of distributed systems is to use multiple computer nodes (hereinafter referred to as "nodes") to improve the processing power of a system to levels higher than a single computer is capable of, or to increase availability. Distributed systems involve more than simply setting up multiple computers, also requiring technology for coordinating their operation.

Large quantities of data must be collected in the cloud, because it is expected to handle the storage and processing of vast amounts of data efficiently. Availability requirements are also increasingly rigorous. Large-scale distributed systems are becoming an extremely important element of cloud computing.

3.3 Examples of Distributed Systems

Distributed systems are a field in which technical development is currently being carried out actively. Here are several well-known examples.

- Google File System (GFS)
  This is a distributed file system created by Google for handling large quantities of high-volume data. Its implementation has not been revealed outside Google. (http://labs.google.com/papers/gfs.html)
- MapReduce
  A framework for large-scale distributed processing devised by Google (details described later). (http://labs.google.com/papers/ mapreduce.html)

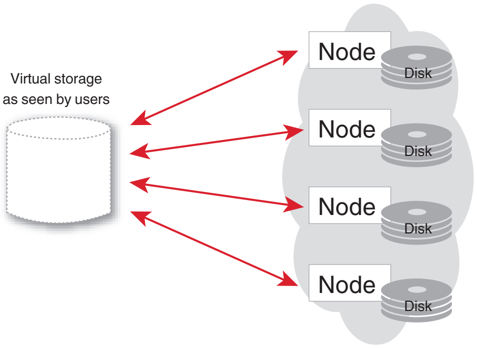


Figure 1: Distributed Storage

Stored data is distributed between multiple nodes. This appears as a single storage device to users.

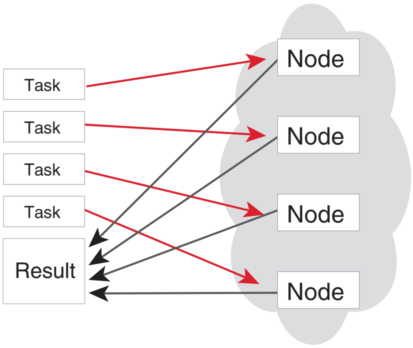


Figure 2: Distributed Data Processing

Data to be processed is divided into many tasks, and processed in parallel using multiple nodes.

- Amazon Dynamo
  A distributed key-value store developed by Amazon. Its implementation has also not been made public. (http://www.allthingsdistributed. com/2007/10/ amazons_dynamo.html)
- Hadoop
  This is a distributed system that was created using the above GFS and MapReduce systems as a reference. It is written in Java, and published as open source software. (http://hadoop.apache.org/)

Of these systems, Google File System and Amazon Dynamo are categorized as distributed storage, and MapReduce is categorized as distributed data processing technology. The ddd service that IIJ has developed incorporates both of these functions.

3.4 History of DDD Development

"ddd" is an abbreviation of "distributed database daemon," and was created to analyze the enormous volume of traffic that flows through the IIJ backbone.

Internet service providers (ISPs) obtain and analyze backbone router traffic information to operate their backbone in a stable manner. In many cases, the counter value for each router interface is obtained via SNMP and converted into a graph. However, as it is not possible to gauge traffic conditions from simple interface IN/OUT information alone, there may be inadequacies with regard to monitoring and analysis.

For this reason, more detailed traffic information known as flow information is used. Some high-end routers and switches used in ISP backbones are capable of outputting flow statistics which include the source of packets, the IP addresses of destination, and port numbers. By obtaining and analyzing this information, it is possible to monitor the status of communications in a level of detail that SNMP cannot capture.

For example, Figure 3 is a graph that indicates traffic color-coded by destination AS number based on flow information. There is a sudden drop in traffic at the right edge of the graph, and when this is analyzed using flow information, it is possible to determine that communications to only a portion of AS have decreased. As only the total traffic volume can be ascertained using SNMP, when it is difficult to identify the cause of anomalies or status changes, flow information can make a detailed analysis possible.

One issue with analyzing flow information is the enormous quantities of data to be handled. While it makes the detailed analysis of communication content possible, the amount of data to be handled also inevitably increases. Generally, flow information is aggregated to some extent immediately after it is received, and then stored after the volume of data is reduced. For example, one method involves aggregating information in source address units, and only storing the total value. However, aggregate values make it impossible to perform a detailed analysis at a later stage, so at IIJ we preserve almost all flow information, and only extract or aggregate information when necessary. For ISPs such as IIJ that operate a large number of network equipment, this method makes the handling of extremely large data necessary.

Previously, IIJ stored flow information in a standard relational database. However, although each record in flow information is small, in the space of five minutes anywhere from hundreds of thousands to millions of records can be generated, so only information for a very short period of time can be stored using a traditional database.

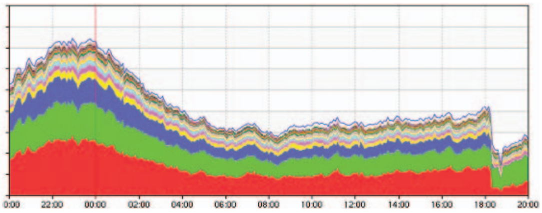


Figure 3: Graph Showing Traffic Color-Coded by AS Number

To handle enormous amounts of flow information over a long period of time, IIJ decided to develop a proprietary distributed system. The result is “ddd”. It can store more than tens of billions of flow information records, and sample and aggregate data at high-speed using a variety of criteria.

The development of ddd began with the handling of flow information as the primary goal, but currently it is applied to a wider range of data processing, such as log analysis for security and application services, and analysis of internal and external security information.

3.5 Overview of DDD

“ddd” is a distributed system that IIJ uses internally, which makes high scalability possible while using low-cost PCs.

The characteristics of ddd are as follows.

- A pure P2P configuration with no single point of failure
- Dynamically extensible distributed storage featuring an automatic data redundancy function
- High-speed data processing via MapReduce

Each ddd node uses the three-layered structure detailed below. All nodes have the same structure. (Figure 4)

Each item is explained in order below.

3.5.1 Pure P2P

Each ddd node forms part of a pure P2P network with no central administrative host. As there is no central administrative host, there is no single point of failure. Each node is equal, and operates in coordination with others. When combined with the data redundancy features described later, the entire system will operate without issue regardless of the time a failure occurs or the specific node it occurs in.

When adding a new node, it is connected to any existing node and booted up. The new node obtains information such as the IP addresses of other nodes from the existing node it is connected to. At the same time, information about the new node is broadcast to other existing nodes.

While ddd is running, it exchanges information with other nodes every few seconds. This means that each node has information about all other nodes. A group of nodes that share information with each other like this is called a cluster.

3.5.2 Distributed Storage

■Key-Value Store

The storage portion of ddd is classified as a distributed key-value store. A distributed key-value store is a type of simple database that stores data as a combination of key and value, and manages these across multiple nodes.

Key-value stores have more limited features compared to existing relational databases (RDB), and have no function for combining data (JOIN) or mechanism for preserving the consistency of transactions. Basically, they only allow a key to be specified, and the corresponding value read or written.

While having limited features, they are ideally suited for distribution across nodes designated according to key value, and as this increases scalability, they are sometimes referred to as the data store for the age of cloud computing.

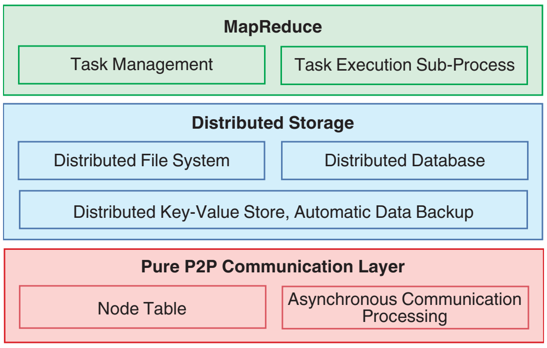

MapReduce
Task Management
Task Execution Sub-Process
Distributed Storage
Distributed File System
Distributed Database
Distributed Key-Value Store, Automatic Data Backup
Pure P2P Communication Layer
Node Table
Asynchronous Communication Processing

Figure 4: Outline of DDD Internal Structure

To designate nodes according to key, ddd uses an algorithm known as consistent hashing.

Consistent hashing treats each node and key as if they are arranged in a hash space on a logical ring (this arrangement is unrelated to the physical network topology of nodes). A node ID is assigned to each node based on its hashed IP address value. The key to be stored is also mapped to the hash space in the same way, and the first node encountered when traveling in a counterclockwise direction is assigned as the storage node of that key for processing. (As SHA-1 is used as the hash function, the size of the hash space is 2 to the power of 160.) Using this method, it is possible to compute the storage node by simply calculating a hash value from the key value, independent of the number of keys stored or the amount of data. (Figure 5)

The largest merit of consistent hashing is that it limits the scope of keys affected when nodes are added or removed. For example, if Node B in the figure below was removed due to failure, the only keys affected would be those indicated by the light green area, with other keys not affected at all. (Figure 6)

In a distributed system environment, it is necessary to consider the routine addition and removal of nodes as a prerequisite. Consistent hashing has the advantage of being flexible when such addition or removal occurs, and it is an algorithm that is often used in distributed key-value stores.

■Automatic Data Redundancy

For redundancy purposes, ddd duplicates all data over three different nodes. Earlier we explained that when using consistent hashing, keys are stored in the first node encountered from their hash value in a counterclockwise direction, but the same data is copied to the second and third nodes encountered as well. In other words, unless all three nodes fail simultaneously, data is preserved on one of the nodes, thereby achieving highly reliable data preservation.

When a node fails, the number of copies of a piece of data temporarily falls to one or two, instead of three (we do not consider a fall to zero likely). To ensure that this situation is not prolonged, ddd copies remaining data to always preserve three copies. To achieve this, ddd uses a system called ihave/sendme, as shown in Figure 7.

First, each node lists the keys that it has stored. As the nodes that should be assigned to a key can be calculated from the key value using consistent hashing, key lists are sent to the corresponding nodes. This is called an ihave message. Nodes receiving an ihave message compare the keys included in the list with the keys they have stored, and if any of the keys are missing, they return a request for that data to be sent. This is called a sendme message. Nodes receiving a sendme message send data to the source that requested it. As there are a large number of keys, key information is exchanged in small batches instead of all at

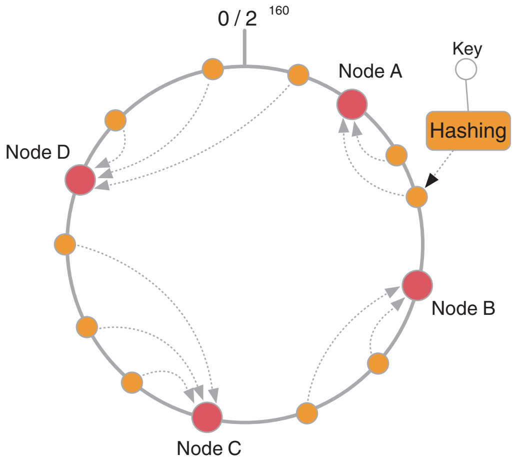


Figure 5: Consistent Hashing - Logical Placement of Keys and Nodes

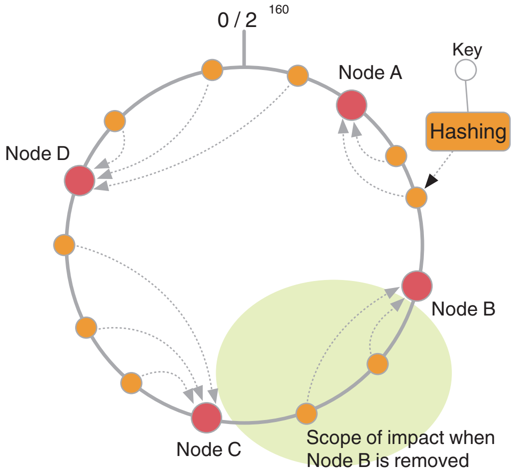


Figure 6: Consistent Hashing - Scope of Impact During Node Failure

once. Additionally, when nodes are added or removed, the ihave destination computed using consistent hashing changes for affected keys only, with data transferred to the newly assigned node. In Figure 6, if Node B was removed, the nodes assigned to the keys indicated by the light green area would change from Nodes B, A, and D to Nodes A, D, and C, and data would be transferred from either A or D to the newly assigned C. This cycle is repeated endlessly in ddd, and as a result, three copies of data are preserved with only a small amount of lead time.

In order to keep the hardware costs for nodes low, ddd does not use disk redundancy technology such as RAID. Instead of this, data redundancy is carried out at a higher level, implementing a system that ensures smooth operation regardless of when a node fails or is removed.

Meanwhile, as the same stored data is distributed over multiple nodes using distributed storage, it is not always possible to preserve the consistency of data. In distributed systems with multiple nodes connected over a network, some nodes may fail or be cut off from the network. Not being able to guarantee consistency is a necessary trade-off for maintaining high availability under these circumstances. In many cases inconsistencies occur for only very short periods, and the system has mechanisms for maintaining consistency over the course of time, but there is also a need for inconsistencies to be dealt with on the application side.

IIJ stores data such as the aforementioned flow information and logs for each server on ddd distributed storage, using the equipment ID and time as keys. Flow information and log information details remain constant, so there is no need to update the information that has been written. Because of this, the previously mentioned characteristic of lacking guaranteed consistency is very rarely a problem. However, there is the possibility of data not being present in a node that it should be stored on during the moment when data is copied after a node is added or removed. In this case, applications using ddd will try to obtain the data from the second and third candidate nodes.

3.5.3 MapReduce

MapReduce is a programming model for large-scale data processing devised by Google. As evident from its name, under this model data is processed in two phases: the map phase and the reduce phase. When used correctly, it makes efficient distributed parallel processing over multiple nodes possible. (Figure 8)

The source code for Google's MapReduce has not been made public, but a paper on its structure has been published by Google. Today a number of implementations with similar functions based on it have appeared, and are being used for tasks such as indexing search engines and analyzing log files. A MapReduce function is also used in ddd for processing distributed storage data.

Another way of describing "map" and "reduce" is "filter" and "aggregate." During the map (filter) phase, necessary information is filtered from data, and converted into a format that makes subsequent processing easier when required. During the reduce (aggregate) phase, mapped information is aggregated. When there are no dependencies between the information to process, processing can be shared over multiple nodes executed in parallel.

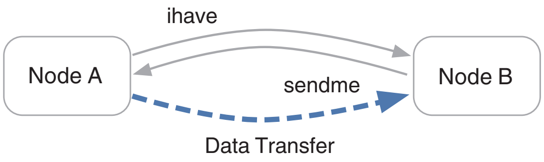


Figure 7 ihave/sendme System

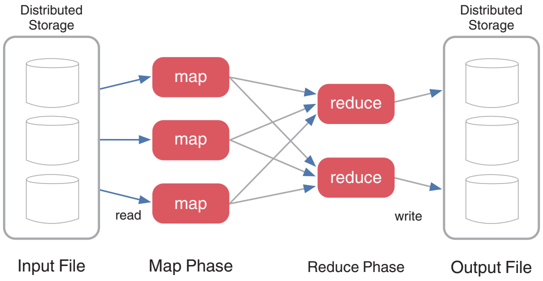


Figure 8: MapReduce Concept

The simplest and easiest to understand application of MapReduce is distributed grep. Grep is a command associated with Unix-based OSes that searches for and outputs lines in a file that match a specified pattern. Because grep performs a round-robin search each time instead of creating a search index in advance, it can be time consuming when used with large files or with many files at once. As grep processing of target files can be shared over multiple nodes when MapReduce is used, users can expect the total processing time to be reduced.

As mentioned previously, flow information and logs output by servers are stored on distributed storage at IIJ, and MapReduce is used to filter and process data. A diverse combination of parameters can be used to analyze this data, and we have constructed a system that makes it possible to analyze data using a variety of parameters according to the type of analysis.

Below we explain the actual behavior of MapReduce using the analysis of flow information as an example.

- A MapReduce job request is prepared, including parameters such as the routers to analyze, the target period, the filtering criteria, and the axis to group.
- The client sends the MapReduce job request to a ddd node.
- The node receiving the request breaks down the MapReduce job into multiple map tasks and reduce tasks, dividing the target period into fixed intervals of time.
- The map tasks are assigned to each node, and each node processes filtering and grouping in accordance with the parameters.
- Once execution of the map tasks on each node is complete, the reduce task is initiated and results are aggregated.
- The aggregated results are written to distributed storage. It is also possible to return them to the client.

Using systems such as this, it is often only possible to retain data for an extremely short period, and analysis can take a long time. However, by using a distributed system made up of many nodes at IIJ, we have made it possible to analyze data from long periods of time with a practical response time.

3.6 Conclusion

Here, we explained the ddd distributed system developed by IIJ. Using ddd it is possible to retain and process large amounts of data. In the future, it is conceivable that provider infrastructures will handle even larger volumes of data. IIJ will continue to develop ddd and provide reliable services as a social infrastructure.

Author:
Takahiro Maebashi
System Development Section, System Infrastructure Division, IIJ Service Business Department
Mr. Maebashi works on the development of programs related to IIJ backbone network operation, starting with the implementation of ddd.

4 Messaging Technology

Previously this was published as the “Email Technical Report.” From this volume we have changed the name to “Messaging Technology.”

4.1 Introduction

Messaging Technology summarizes the latest trends in spam, technical countermeasures to spam, etc. For trends in spam, the results of a variety of analyses conducted based on various information obtained from the Spam Filter feature provided in IIJ email services will be presented. Since the flow of email varies depending on the day of the week, in order to more easily understand the trends, the data was aggregated in one-week units and analyzed focusing on the changes in the data.

This survey covers a period of 13 weeks or 91 days, from the 14th week of 2009 (3/30/2009 to 4/5/2009) to the 26th week (6/22/2009 to 6/28/2009).

Regarding trends in email technologies, we explain the implementation status of sender authentication technologies on the receiving side, and examples of DKIM usage.

4.2 Trends in Spam

This section provides a report focused on the trends in the ratio of spam detected by the Spam Filter feature provided by IIJ and analysis results related to sources of spam.

4.2.1 Ratio of Spam

The weekly trends in the ratio of spam over a period of 91 days from the 14th week of 2009 to the 26th week are shown in Figure 1. The ratio of spam averaged 81.6% of all incoming emails during this period. The average value was almost the same level as the previous period (81.5%), but for this period several distinct changes in the ratio trends were observed. The ratio was highest during the 19th week (5/4/2009 to 5/10/2009) at 87.1%.

Similarly to previous trends, as this period includes a series of public holidays in May, the volume of general business email was lower, and due to this the relative ratio of spam increased. However, from this period actual volumes of spam received also increased dramatically. In particular, spam increased from the 18th week (4/27/2009) to the 22nd week (5/25/2009), trending at a high ratio of over 80%.

Following this, spam entered a slight declining trend from the 23rd week (6/1/2009). During this period, the US Federal Trade Commission announced on June 4, 2009[*1] that they had shut down network access for Pricewert LLC, an ISP, which had become a hotbed of spyware, phishing, and child pornography. Pricewert also did business under the names such as 3FN and APS Telecom, and also reportedly operated servers for controlling botnets (command and control servers), similar to McColo[*2], which was shut down in November, 2008. It is believed that the shutdown of Pricewert's network weakened botnet activity, and reduced spam volume. However, as a dramatic decrease of the magnitude of the McColo case[*3] was not observed, it is conceivable that either the affected botnets were of a small scale, or the sender had knowledge of the shutdown in advance, and took some form of remedial measures.

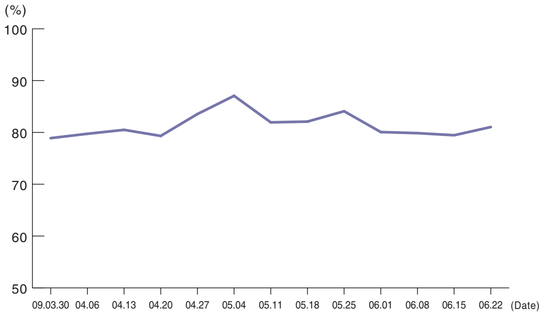


Figure 1: Ratio Proportion of Spam

[*1] http://www.ftc.gov/opa/2009/06/3fn.shtm.

[*2] Explanation in IIR Vol.2 (http://www.iij.ad.jp/development/iir/pdf/iir_vol02_mail.pdf).

[*3] In the 47th week of 2008 (11/17 to 11/23), the ratio of spam dropped to 68%.

4.2.2 Sources of Spam

Figure 2 shows the source countries of spam during this period.

In this survey, as in the previous one, the top source of spam was Brazil (BR), accounting for 11.8% of the total. This is a slight increase over the previous survey, in which Brazil accounted for 11.3% of total spam. The United States ranked 2nd (US) at 11.4%, the same ranking it held for the previous survey (Vol.3, 10.9%), and the survey before that (Vol.2, 14.4%).

In the current survey results, the gap between the top two countries and those ranked 3rd and below increased slightly. China ranked 3rd (CN, 6.9%), South Korea 4th (KR, 5.6%), Turkey 5th (TR, 5.4%), and India 6th (IN, 5.3%). Comparing these results with those from the previous survey, there are a few changes in ranking, but the top six countries remain the same. Japan (JP, 2.6%) was ranked 11th, the same ranking it held in the previous survey.

The weekly trends in the ratio of spam from these 6 countries and Japan are shown in Figure 3. Brazil maintains a high ratio each week, but we can see that the ratio for the United States drops after mid-May. The ratio of spam from China has dropped slightly since it ranked in 1st place in the survey before last (Vol.2), but it has been gradually returning to a high level since June, so caution is once again required.

As the majority of spam sent to Japan is sent from overseas, we believe that the international coordination of anti-spam measures is essential.

4.2.3 International Anti-Spam Measure Trends

As can been seen from the data we have presented, high volumes of spam are still being sent. The same trend can be seen both in Japan and internationally. It is said that the source of most spam is bots that infect Consumer PCs with malware, and control them from outside the network.

Japan has constructed an environment that prevents spam being sent using bots such as these through the widespread implementation of OP25B[*4], which restricts the sending of email directly to external networks from dynamic IP addresses. Japan is not the first country to introduce OP25B technology, as some ISPs including major ones in the United States have already introduced it. After the establishment of the MAAWG[*5] group for combating international spam, OP25B received attention as an effective technology for defending against senders of spam. After intensive discussions, Japan's JEAG[*6] published a recommendation for OP25B[*7], and due to this it was rapidly adopted in Japan.

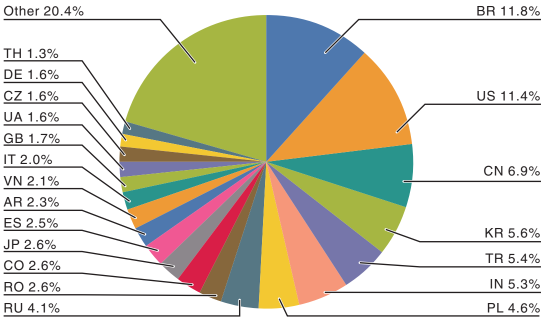


Figure 2: Sources of Spam

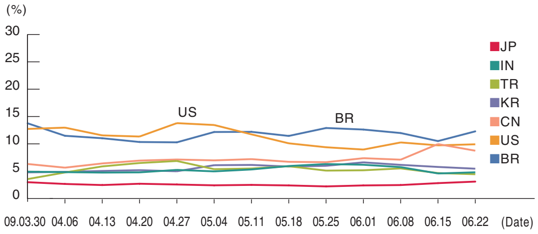


Figure 3: Trends in Sources of Spam

[*4] Outbound Port 25 Blocking

[*5] See Internet Topics for more information about MAAWG (Messaging Anti-Abuse Working Group).

[*6] JEAG (Japan Email Anti-Abuse Group) is a working group founded by Japan's major Internet service providers (ISPs) and mobile telecommunication carriers to counter spam email abuse (http://www.iij.ad.jp/en/news/pressrelease/2005/0315.html).

[*7] See "The Japan Email Anti-Abuse Group (JEAG) Drafts Recommendations on the Fight against Spam E-mail" at the following URL. (http://www.iij.ad.jp/en/news/pressrelease/2006/0223.html).

It should be possible to reduce the volume of spam that Japan receives from overseas through the adoption of OP25B in wider areas. For this reason, IIJ has continued its efforts to accelerate the introduction of OP25B, advocating its effectiveness and presenting a technological overview of it to other countries through opportunities such as MAAWG international conferences and activities in coordination with the government. OP25B has been introduced in some areas as a result, but in many areas progress towards its introduction is faltering for a number of reasons. We will explain the details of this on another occasion, and we plan to continue pushing for the introduction of OP25B.

Regarding trends in countermeasures against senders of spam, moves to shut down networks thought to be controlling botnets continue in the United States, as evidenced by the network shutdown of McColo in November, 2008, and Pricewert in June, 2009. Shutting down communications from the control source that sends commands to bots certainly has a greater temporary impact than disinfecting each bot individually. However, there is a possibility that the controllers of botnets that send spam have implemented countermeasures of their own, and have already introduced new technology, as the impact of Pricewert's recent shutdown seemed to be limited. There have already been reports*[8] of the existence of new botnets that transmit commands using peer-to-peer technology, with no specific control source. As long as the sending of spam remains a viable business practice, it is conceivable that this kind of innovation of sending methods will continue.

Recently, some telecommunications carriers have introduced a technique called Walled Garden*[9] as a countermeasure against the senders of spam. Walled Garden is a technique for isolating communications from users thought to be sending spam in a specific location, instead of passing them through to the Internet directly. This makes it possible to analyze bot behavior, and implement security measures by alerting general users who are unintentionally carrying out unauthorized communications because of a malware infection. For example, by guiding all Web access (HTTP/HTTPS) to a specific page, it is possible to suggest the use of Windows Update or the execution of anti-virus software, and prevent the PC from connecting to the Internet until it is cleaned. However, there are many issues with the Walled Garden technique, such as the identification of sources that are behaving suspiciously, and the preparation of a system for responding to inquiries from users who have been guided to Walled Garden.

OP25B can suppress the sending of spam, but it cannot respond to DDoS attacks that use bots, for example. Recently, there have been incidents of government-related Websites in the United States and South Korea becoming inaccessible, and reports suggest that botnets were responsible for these attacks. Because of this, we believe that the introduction of OP25B is not enough, and that efforts to maintain a clean network environment by combining OP25B with the Walled Garden technique are necessary.

*8 HotBots'07 (http://www.usenix.org/events/hotbots07/tech/).

*9 MAAWG has published their best practices for Walled Garden (http://www.maawg.org/about/whitepapers/MAAWG_Walled_ Garden_BP_2007-09.pdf).

4.3 Trends in Email Technologies

4.3.1 Trends in Sender Authentication Technologies

The WIDE project survey results*[10] that we have also cited several times in the past provide insight into the implementation status of sender authentication technologies on the sending side for the Japan domain ("jp" domain). These results allow us to confirm the implementation ratio on the sending side, and in particular the high rate of publication of SPF records (3.99% as of August, 2009). Meanwhile, let us look at how the implementation of sender authentication technologies is progressing on the email receiving side.

The Japan Data Communications Association has carried out a survey of sender authentication technology implementation status, targeted at businesses such as ISPs and mobile telecommunication carriers that provide email services to a wide range of consumers, and published the results*[11]. According to the survey results, as of July 2, 2009, 13 of the 41 companies that participated in the survey were carrying out receiving-side authentication using SPF (Sender Policy Framework) or SenderID. This comes to a ratio of approximately 31.7%, or an even lower penetration rate of approximately 22.6% when data is limited to ISPs. The implementation ratio of DKIM on the receiving side was lower still, at approximately 14.6%.

Many enterprises did not participate in this survey, and the volume of email and number of accounts handled by each participant vary, so this is not a straightforward indication of the penetration rate of sender authentication technologies. However, given that this survey was targeted at telecommunications carriers, our honest impression is that these numbers are lower than they should be. New functions must be added in order to carry out authentication on the receiving side, so a clear-cut comparison cannot be made, but the results compare extremely unfavorably with the high penetration rates seen on the sending side. We believe that to accelerate implementation on the receiving side there is a need to further clarify the effects and benefits of implementation.

4.3.2 About DKIM Usage

In our last report we gave an overview of the DKIM authentication structure and processing on the sending and receiving sides. This time, we will explain the benefits and practical applications of DKIM.

DKIM authenticates the sender of an email by attaching a digital signature that cannot be created unless the sender has the private key. The digital signature is created from the email body and headers, so as long as the source information is not changed, verification is possible at any time provided that the public key for verifying the signature can be obtained. This means that unlike network-based SPF/SenderID, there is no chance of authentication failing due to email being forwarded. This is a significant advantage of DKIM.

Conversely, one case in which DKIM authentication fails is when a mailing list name or counter is added to the Subject header in a mailing list. The addition of strings such as this constitutes modification of the email, so the digital signature does not match, and authentication fails. This is often brought up as one of the disadvantages of DKIM.

However, currently most mailing lists already add information to the Subject header and change sender information in advance, making them a system for redelivering email to mailing list members, rather than simply a way to process the forwarding of email. In other words, mailing list systems become the sender of email to be delivered, and from the perspective of DKIM, we believe that signatures should be attached on the mailing list system side to begin with. For this reason, we recommend avoiding the issue of DKIM authentication failing due to mailing lists by creating digital signatures at the time of delivery.

*[10] Survey Results on Deployment Ratio of Sender Authentication Technologies published by WIDE (http://member.wide.ad.jp/wg/antispam/stats/index.html.en).

*[11] Sender Authentication Implementation Status (http://www.dekyo.or.jp/soudan/auth/).

There is another benefit of making DKIM digital signature authentication possible from the email body alone. For example, when the sender of a mail magazine receives feedback such as subscription cancelations or suggestions for improvement, they will generally want to confirm that the user is the recipient of the mail magazine. In this case, if the sender of the mail magazine attaches a DKIM digital signature at the time of delivery, users sending feedback can attach the email that was originally sent to reauthenticate the attached email, making it possible to confirm whether or not they really sent the email. Additionally, IETF has published ARF (Abuse Reporting Format), which can also be used as a format for feedback such as this, as an Internet Draft, and its standardization is being discussed. (Figure 4)

4.4 Conclusion

In this volume's Messaging Technology, we introduced recent trends in countermeasures against senders of spam, such as countermeasures against controllers of botnets, and the Walled Garden technique that is gaining momentum as a defense against spam senders alongside OP25B. The sending of spam is a business for those who send it, and they are innovating technology on a daily basis to devise new ways of ensuring their spam is delivered. Comprehensive countermeasures that encapsulate the sending and receiving of email and best practices for network management are becoming necessary. We will continue to introduce such countermeasure technologies in this whitepaper in the future.

We are faced with the fact that, compared with SPF/Sender ID that only requires an SPF record to be set and published one time, implementation of DKIM is not progressing very rapidly. It is conceivable that cost-effectiveness is one the factors behind this, so we would like to continue to promote the implementation of DKIM by introducing its merits and utilization methods.

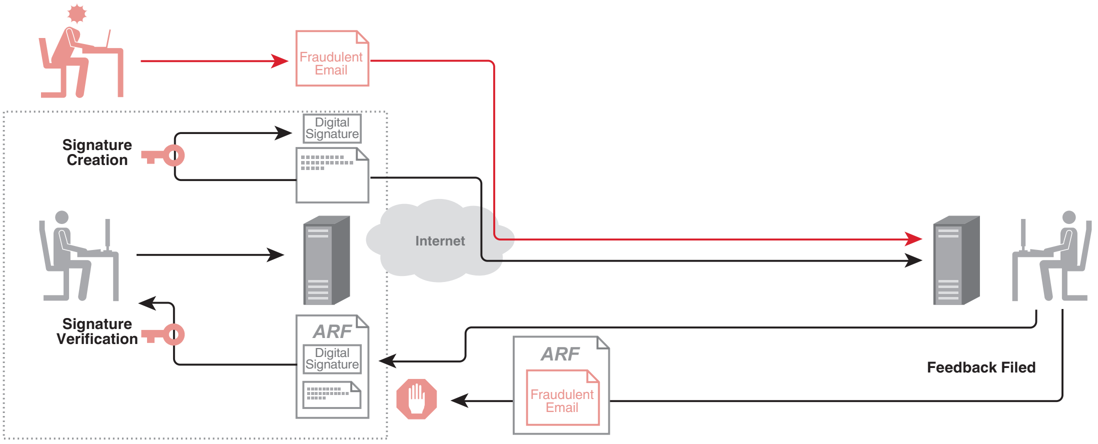


Figure 4: Example of Using DKIM with ARF

Author:
Shuji Sakuraba
Shuji Sakuraba is a Senior Program Manager in the Service Promotion Section of the Messaging Service Division in IIJ Network Service Department. He is engaged in the research and development of messaging systems. He is involved in various activities in collaboration with external related organizations for securing a comfortable messaging environment. He is a MAAWG member and JEAG board member. He is a member of the Council for Promotion of Anti-Spam Measures and administrative group. He is also a member of Internet Association Japan's Anti-Spam Measures Committee.

Internet Topics: Messaging Anti-Abuse Working Group

■About MAAWG

With global spam on the increase, IIJ was among the 19 international telecommunications carriers and ISPs who established MAAWG (Messaging Anti-Abuse Working Group)[*1] on January 19, 2004[*2]. As a founding member of MAAWG, IIJ has participated in MAAWG activities for the past five years. Here will we introduce the details of MAAWG activities and present a summary of the 16th General Meeting held in June, 2009.

MAAWG members include a variety of companies involved with email, such as major ISPs, ESPs (Email Service Providers), and email delivery contractors and vendors. As of the end of 2008, the number of members has risen to 161 companies. The main activities of MAAWG involve countermeasures against the unauthorized use of email to spread spam and viruses. In recent years, however, many issues such as countermeasures against botnets that are the source of such problems and the malware (unauthorized programs) behind these botnets have also become topics of discussion. As a result of its activities, MAAWG has published a variety of documents such as recommendations, best practices, and whitepapers. These are also made available to non-members, and can be obtained from the MAAWG Website.

A wide variety of companies involved with email currently participate as MAAWG members. Members participate in discussions covering a number of fields, such as the Technical Committee for discussing technical matters, the Collaboration Committee for discussing operational issues, and the Public Policy Committee that carries out activities such as coordination with law enforcement agencies and international organizations. Another characteristic of MAAWG is the variety of discussions that are held based on a specific theme or on the role of participants, such as the Senders SIG for sender organizations or the ISP Closed Colloquium for which participation is limited to ISPs.

MAAWG members meet face-to-face at the General Meeting that is held three times each year, but in addition to this also share information and opinions on published documents on an everyday basis using a mailing list. An Abuse Contact Database has also been created so that members can contact each other directly, and this contributes to improving the international email environment through its use to confirm status when the transmission of email between ISPs is not going smoothly.

■16th MAAWG General Meeting

The General Meeting is a precious opportunity for MAAWG members to meet each other face-to-face. In recent years they have been held around February and October in North America, and in June in Europe. Here we will present the details of the 16th General Meeting held in Amsterdam in the Netherlands from June 8 to June 11.

When MAAWG was established there were open sessions in which anyone could participate, but currently only MAAWG members and invited guests can participate in the meeting. As making details of the meeting public is prohibited, we cannot discuss the details of each session, but we will present a summary.

The meeting held in Europe, partly due to it being the headquarters of international organizations such as the ITU and the OECD, tends to be higher participation from those involved in government. A large number of organizations were in attendance at this meeting, such as the Council of Europe and Europol, the United States FTC and the Netherlands OPTA (Independent Postal and Telecommunication Authority), with each presenting information about the initiatives they are undertaking. This year there was a record number of attendees for the meeting held in Europe, with over 270 individuals from 19 countries participating, demonstrating the high level of interest and also the seriousness of the issues faced in this field.

The General Meeting is normally held over three days, with sessions on a variety of topics continuing from 8:30 A.M. to 6:00 P.M. Most sessions are related to email, and as multiple sessions are held concurrently, participants spend most of the day cooped up in the hotel that serves as the meeting place. Social events are also held to cultivate friendships between members, and this is an opportunity to meet out of the hotel and discuss solutions to everyday problems and for collaborations between companies.

JEAG (Japan Email Anti-Abuse Group)[*3], which counters spam e-mail abuse in Japan, was founded after the establishment of MAAWG. JEAG also coordinates with MAAWG, with JEAG members participating in MAAWG General Meetings as guests, and introducing JEAG's activities and initiatives in Japan. As a founding member of both, IIJ will continue to be extremely active, serving as a bridge between Japan and international organizations.

Author:
Shuji Sakuraba
Shuji Sakuraba is a Senior Program Manager in the Service Promotion Section of the Messaging Service Division in IIJ Network Service Department.

[*1] http://www.maawg.org/

[*2] http://www.iij.ad.jp/news/pressrelease/2004/0119.html

[*3] http://www.jeag.jp/

Ongoing Innovation

About Internet Initiative Japan Inc. (IIJ)

IIJ was established in 1992, mainly by a group of engineers who had been involved in research and development activities related to the Internet, under the concept of promoting the widespread use of the Internet in Japan.

IIJ currently operates one of the largest Internet backbones in Japan, manages Internet infrastructures, and provides comprehensive high-quality system environments (including Internet access, systems integration, and outsourcing services, etc.) to high-end business users including the government and other public offices and financial institutions.

In addition, IIJ actively shares knowledge accumulated through service development and Internet backbone operation, and is making efforts to expand the Internet used as a social infrastructure.

Internet Initiative Japan Inc.
Address: Jinbocho Mitsui Bldg., 1-105 Kanda Jinbo-cho, Chiyoda-ku, Tokyo, 101-0051
Email: info@iij.ad.jp URL: http//www.iij.ad.jp/