Internet Infrastructure Review

IIJ
Internet Initiative Japan

Vol.9

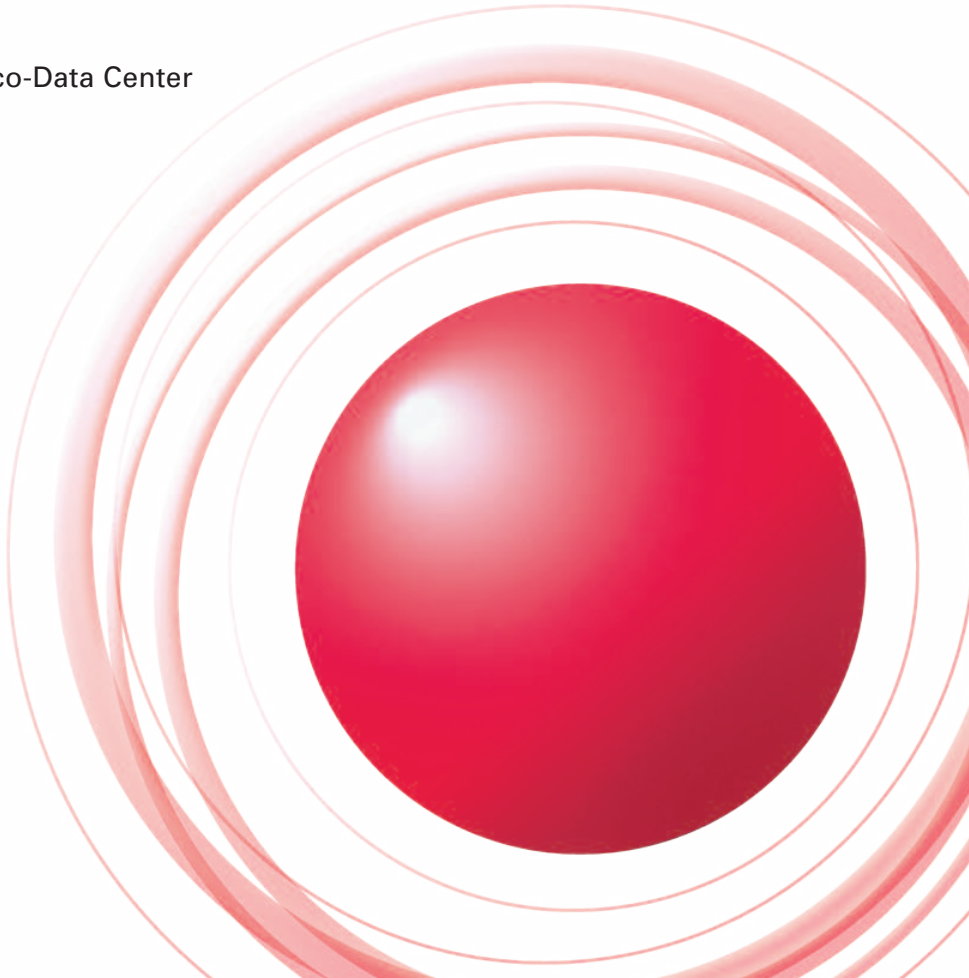
November
2010

Infrastructure Security
Preparing for DDoS Attacks

Internet Operation
Steps Towards Implementing DNSSEC

Messaging Technology
Sender Implementation of Sender Authentication Technology Sluggish

Modular Eco-Data Center
A Report on Proof-of-Concept Tests
for our Next-Generation Modular Eco-Data Center



Internet Infrastructure Review Vol.9 November 2010

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

Executive Summary

With the shift toward cloud computing over the last few years, it seems as if the Internet has evolved beyond merely serving as an open and simple network system for telecommunications, and is now playing a deeper role in today's advanced information society in a variety of contexts, incorporating information systems that were once outside the network as well as the information services realized through them.

According to a report published by the Ministry of Internal Affairs and Communications' Smart Cloud Study Group in May of this year, while 56.2% of businesses in the United States use cloud computing, businesses in Japan are lagging behind with just 14.8% utilizing cloud technology. However, the same report estimates that the market for cloud computing in Japan will expand, growing by a factor of 3.2 compared to 2010 levels to approximately 2.4 trillion yen in 2015.

Against this background we are reaching the point where consideration must be given to future developments, with the Internet transforming from a simple network infrastructure into an infrastructure that encompasses all manner of information systems.

Since last year IIJ and a number of other providers have launched cloud services, with business on these platforms swinging into action, and the development and construction of the systems, equipment, and infrastructure necessary to provide them starting to move forward. At the same time, it is also becoming more and more crucial to secure the stability and reliability of the networks that serve as the infrastructure for cloud services.

This report discusses the results of the various ongoing surveys and analysis activities that IIJ carries out to maintain and develop the Internet infrastructure and enable our customers to continue to use it safely and securely. We also regularly present summaries of technological development as well as important technical information.

In the "Infrastructure Security" section, we report on the results of our ongoing statistics gathering and analyses for security incidents observed during the three months from July 1 to September 30, 2010. We also present our focused research for this period, examining the preparations to be made for DDoS attacks on small-scale systems and security for shared systems such as cloud computing, as well as giving an overview of digital forensics.

In the "Internet Operation" section, we comment on technology known as DNSSEC that enables verification of responses from DNS, a service essential to the use of the Internet, and also look at the steps necessary when introducing this technology.

In the "Messaging Technology" section, we examine spam ratio trends and regional source distribution, as well as trends in the main regional sources of spam, for the 13 weeks between the end of June and the end of September, 2010. Additionally, in "Trends in Email Technologies," we report on the implementation status of sender authentication technologies and the current state of botnet countermeasures.

In the "Modular Eco-Data Centers" section, we provide a detailed explanation of the test system configuration and results of the proof-of-concept tests carried out for the development of IIJ's next-generation modular eco-data center, which uses container units with an outside-air cooling system.

IIJ will continue to publish periodic reports covering information such as this, and provide customers with a variety of solutions for the stable, secure, and innovative use of the Internet as an infrastructure for supporting corporate activities.

Author:
Toshiya Asaba
President and CEO, IIJ Innovation Institute Inc. Mr. Asaba joined IIJ in its inaugural year of 1992, becoming involved in backbone construction, route control, and interconnectivity with domestic and foreign ISPs. He was named IIJ director in 1999, and as executive vice president in charge of technical development in 2004. Mr. Asaba founded the IIJ Innovation Institute Inc. in June 2008, and became president and CEO of that organization.

Preparing for DDoS Attacks

In this report, we will explain incidents that occurred between July and September 2010, and also examine preparations to be made for DDoS attacks on small-scale systems, discuss security considerations for shared systems such as those on cloud computing environments, and give an overview of digital forensics.

1.1 Introduction

This report 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 with which IIJ has cooperative relationships. This volume covers the period of time from July 1 through September 30, 2010. In this period a number of vulnerabilities related to Web browsers and their plug-ins continued to be exploited. There were also incidents that led to financial damages in which SIP was exploited to make toll calls, and in September a series of synchronized attacks on multiple Web servers in Japan occurred in response to the social situation. 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 July 1 and September 30, 2010. Figure 1 shows the distribution of incidents handled during this period*1.

■ Vulnerabilities

During the period a large number of vulnerabilities were discovered and fixed in Microsoft Windows*2*3*4*5 as well as applications such as Adobe Systems' Adobe Reader and Acrobat*6*7, Adobe Flash Player*8*9, and Apple's QuickTime*10. Several of these vulnerabilities were exploited before patches were released. A vulnerability in the Linux kernel*11 was also patched. Fixes were also made to vulnerabilities in server applications such as BIND DNS servers*12, and ISC DHCP servers*13, in addition to a number of vulnerabilities in router products such as Cisco Systems' Cisco IOS*14*15. Vulnerabilities were also patched in Apple's iOS*16, which is used as firmware for devices such as mobile phones.

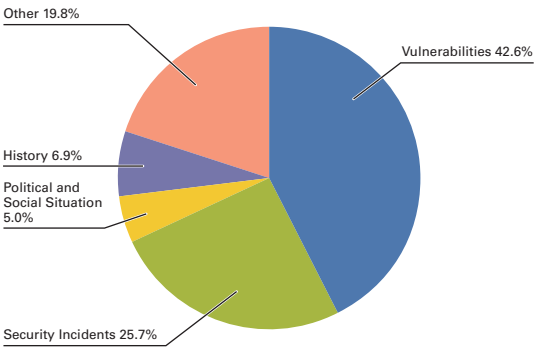


Figure 1: Incident Ratio by Category (July 1 to September 30, 2010)

■ Political and Social Situations

IIJ pays close attention to various political and social situations related to international affairs and current

*1 Incidents discussed in this report are categorized as vulnerabilities, political and social situation, history, security incident and other. Vulnerabilities: Responses to vulnerabilities associated with network equipment, server equipment or software used over the Internet, or used commonly in user environments. Political and Social Situations: Responses to incidents related to domestic and foreign circumstances and international events such as international conferences attended by VIPs and attacks originating in international disputes. History: Historically significant dates; warning/alarms, detection of incidents, measures taken in response, etc., related to attacks in connection with a past historical fact. Security Incidents: Wide propagation of network worms and other malware; DDoS attacks against certain websites. Unexpected incidents and related response. Other: Security-related information, and incidents not directly associated with security problems, including highly concentrated traffic associated with a notable event.

*2 Microsoft Security Bulletin MS10-042 - Critical: Vulnerability in Help and Support Center Could Allow Remote Code Execution (2229593) (http://www.microsoft.com/technet/security/bulletin/ms10-042.mspx).

*3 Microsoft Security Bulletin MS10-046 - Critical: Vulnerability in Windows Shell Could Allow Remote Code Execution (2286198) (http://www.microsoft.com/technet/security/bulletin/ms10-046.mspx).

events. During this period we turned our attention to the incident in which a Chinese boat collided with Japan Coast Guard patrol vessels in early September.

History

The period in question included several historically significant days on which incidents such as DDoS attacks and website alterations have occurred. During the period for the current report there were warnings of an attack on September 18 (the date of the Manchurian Incident), and we paid close attention to our equipment and our customer networks for attack behavior. Attacks linked to this incident included DDoS attacks and alteration attempts against the websites of a number of organizations related to government agencies, general companies, and unrelated associations.

Security Incidents

Unanticipated security incidents not related to political or social situations were discovered in the form of malware*17 that targets Siemens' industrial control systems*18. An increase was also observed in the unauthorized SIP communications*19 that have been occurring of late. Additionally, a cross-site scripting vulnerability in Twitter was discovered*20 and exploited*21, and a vulnerability in ad distribution servers was exploited*22 to partially alter data and induce users to download scareware.

Other

Regarding trends for other security-related topics, signature protection for the DNS root zone was put into effect*23 to facilitate the implementation of DNSSEC, and in Japan it was announced that DNSSEC will be implemented for JP domain name services in January 2011*24. Microsoft released a patch*25 implementing RFC5746, which was established due to a vulnerability in the TLS protocol relating to the renegotiation feature. In September there was an activity that set out to release information about unpatched vulnerabilities each day, and this led to a large amount of vulnerability information being made public*26.

*4 Microsoft Security Advisory (2269637) Insecure Library Loading Could Allow Remote Code Execution (http://www.microsoft.com/technet/security/advisory/2269637.mspx).

*5 Microsoft Security Bulletin MS10-070 - Important: Vulnerability in ASP.NET Could Allow Information Disclosure (2418042) (http://www.microsoft.com/technet/security/bulletin/ms10-070.mspx).

*6 APSB10-17 Security updates available for Adobe Reader and Acrobat (http://www.adobe.com/support/security/bulletins/apsb10-17.html).

*7 APSB10-21 Security updates available for Adobe Reader and Acrobat (http://www.adobe.com/support/security/bulletins/apsb10-21.html).

*8 APSB10-16 Security update available for Adobe Flash Player (http://www.adobe.com/support/security/bulletins/apsb10-16.html).

*9 APSB10-22 Security update available for Adobe Flash Player (http://www.adobe.com/support/security/bulletins/apsb10-22.html).

*10 About the security content of QuickTime 7.6.7 (http://support.apple.com/kb/HT4290).

*11 A vulnerability was found in the Linux 64-bit kernel. This information is managed as CVE-2010-3081 (http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2010-3081).

*12 RRSIG query handling bug in BIND 9.7.1 (http://www.isc.org/software/bind/advisories/cve-2010-0213).

*13 DHCP: Fencepost error on zero-length client identifier (http://www.isc.org/software/dhcp/advisories/cve-2010-2156).

*14 Cisco Security Advisory: Cisco IOS XR Software Border Gateway Protocol Vulnerability (http://www.cisco.com/en/US/products/products_security_advisory09186a0080b4411f.shtml).

*15 Cisco Security Advisory: Summary of Cisco IOS Software Bundled Advisories, September 22, 2010 (http://www.cisco.com/warp/public/707/cisco-sa-20100922-bundle.shtml).

*16 About the security content of iOS 4.1 for iPhone and iPod touch (http://support.apple.com/kb/HT4334).

*17 There are many detailed reports related to this malware, for example the following commentary from Nippon CSIRT Association. About the Stuxnet malware (http://www.nca.gr.jp/2010/stuxnet/index.html) (in Japanese).

*18 A form of SCADA (Supervisory Control And Data Acquisition). This is a solution for monitoring systems and controlling processes via computer that is generally used at facilities such as factories.

*19 Fraudulent incoming SIP 24 (http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi?p=%C9%D4%C0%B5%A4%CASIP%C3%E5%BF%AE+24) (in Japanese). cNotes provides SIP observation data on an irregular basis.

*20 Details of this vulnerability can be found in the following official blog post. Twitter blog - All about the "onMouseOver" incident (http://blog.twitter.com/2010/09/all-about-onmouseover-incident.html).

*21 Details of this incident can be found in the following F-Secure blog post. Worms Loose on Twitter.com (http://www.f-secure.com/weblog/archives/00002034.html).

*22 This incident is also detailed in the following Trend Micro blog post. Adobe zero-day attacks and Web-based threats via ad distribution systems - looking back on threat trends for September 2010 (http://blog.trendmicro.co.jp/archives/3700) (in Japanese).

*23 Information about DNSSEC for the Root Zone (http://www.root-dnssec.org/2010/07/16/status-update-2010-07-16/).

*24 JPRS Plans to Implement DNSSEC in JP Domain Name Services in January 2011 (http://jprs.co.jp/en/topics/2010/100728.html).

*25 Fixes regarding the TLS renegotiation feature are included in the following program update. Microsoft Security Bulletin MS10-049 - Critical: Vulnerabilities in SChannel could allow Remote Code Execution (980436) (http://www.microsoft.com/technet/security/bulletin/ms10-049.mspx). This issue is explained in Vol.6 of this report under "1.4.2 MITM Attacks Using a Vulnerability in the SSL and TLS Renegotiation" (http://www.iij.ad.jp/en/development/iir/pdf/iir_vol06_EN.pdf).

*26 MOAUB (Month of Abysssec Undisclosed Bugs). Details of the vulnerabilities reported through this initiative can be found on the Abysssec Security Research blog. MOAUB - Day by Day (http://www.abysssec.com/blog/2010/09/moaub-1/).

1.3 Incident Survey

Of 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 such as that of vulnerabilities, but rather cause large volumes of unnecessary traffic to overwhelm network bandwidth or server processes for the purpose of hindering services.

■ Direct Observations

Figure 2 shows the circumstances of DDoS attacks handled by the IIJ DDoS Defense Service between July 1 and September 30, 2010.

This information shows traffic anomalies judged to be attacks based on IIJ DDoS Defense Service standards.

There are many methods that can be used to carry out a DDoS attack, and the capacity of the environment attacked (bandwidth and server performance) will largely determine the degree of impact. Figure 2 categorizes DDoS attacks into three types: attacks on bandwidth capacity*27, attacks on servers*28, 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 622 DDoS attacks. This averages to 6.76 attacks per day, which is three times the average daily number of attacks observed during the period for our prior report. Bandwidth capacity attacks accounted for 1% of all incidents, server attacks accounted for 72% of all incidents, and compound attacks accounted for the remaining 27%. This is due to a drastic increase in attacks on multiple Web servers that occurred over the period of September 10 to September 30, which made up 46% of the total.

The largest attack observed during the period under study was classified as a bandwidth capacity attack, and resulted in 1.4Gbps of bandwidth using up to 275,000pps packets. Of all attacks, 66% ended within 30 minutes of commencement, while 20% lasted between 30 minutes and 24 hours. The longest attack continued for 12 days (291 hours), and consisted of a compound attack that resulted in 670Mbps of bandwidth using up to 120,000pps packets.

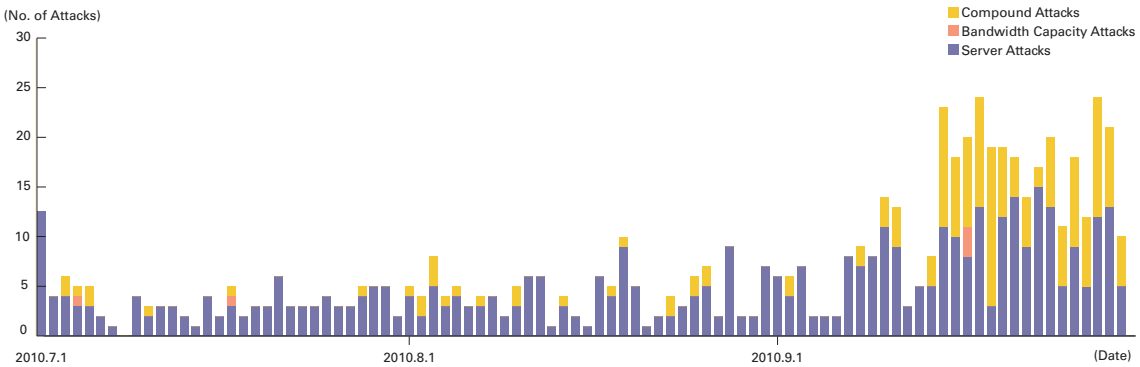


Figure 2: Trends in DDoS Attacks

*27 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.

*28 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.

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*29 and botnet*30 usage as the method for conducting DDoS attacks.

Backscatter Observations

Next we present our observations of DDoS backscatter using the honeypots*31 set up by the MITF, a malware activity observation project operated by IIJ*32. By monitoring backscatter it is possible to detect certain types of DDoS attacks occurring on external networks as a third party without any interposition.

Figure 3 shows trends in packet numbers by port for the backscatter observed between July 1 and September 30, 2010, and Figure 4 shows the sender's IP addresses classified by country.

The port most commonly targeted by the DDoS attacks observed was the 80/TCP port used for Web services, accounting for 58.4% of the total during this period. Attacks on 3389/TCP used for remote desktop were also observed. Additionally, many attacks were observed on ports not used by common applications, such as 5218/TCP and 5224/TCP. Looking at the origin of backscatter thought to indicate IP addresses targeted by DDoS attacks by country in Figure 4, China and the United States accounted for large proportions at 44.8% and 29.5%, respectively, and Japan made up 2.1% of the total. The particularly large number of backscatter packets observed targeting 5224/TCP on August 20 and 5218/TCP on September 19 all show a single IP address in China as the attack target.

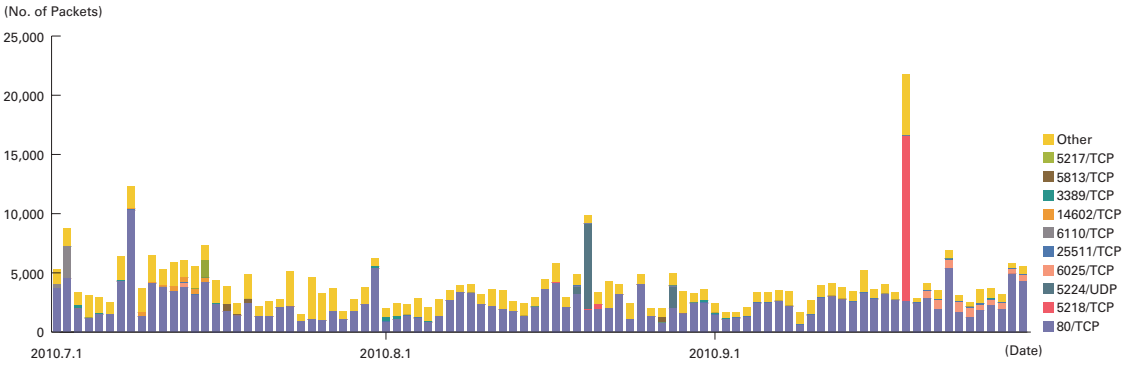


Figure 3: DDoS Attack Backscatter Observations (Observed Packets, Trends by Port)

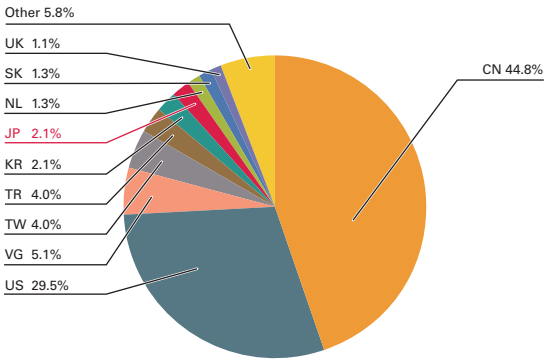


Figure 4: DDoS Attack Target Distribution According to Backscatter Observations (by Country, Entire Period under Study)

*29 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.

*30 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."

*31 Honeypots established by the MITF, a malware activity observation project operated by IIJ. See also "1.3.2 Malware Activities."

*32 The mechanism and limitations of this observation method as well as some of the results of IIJ's observations are presented in Vol.8 of this report under "1.4.2 Observations on Backscatter Caused by DDoS Attacks" (http://www.iij.ad.jp/en/development/iir/pdf/iir_vol08_EN.pdf).

1.3.2 Malware Activities

Here, we will discuss the results of the observations of the MITF*33, a malware activity observation project operated by IIJ. The MITF uses honeypots*34 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 5 shows trends in the total volumes of communications coming into the honeypots (incoming packets) between July 1 and September 30, 2010. Figure 6 shows the distribution of sender's IP addresses by country. The MITF has set up numerous honeypots for the purpose of observation. We have taken the average per honeypot, showing the trends for incoming packet types (top ten) over the entire period subject to study.

Much of the communications arriving at the honeypots demonstrated scanning behavior targeting TCP ports utilized by Microsoft operating systems. We also observed scanning behavior for 1433/TCP used by Microsoft's SQL Server and 23/TCP used for telnet. Additionally, attacks were observed on ports not used by common applications, such as 5121/TCP, 31795/TCP, 23502/TCP, and 9415/TCP. Looking at the overall sender distribution by country in Figure 6, we see that attacks sourced to Japan at 30.4%, China at 15.9%, and Taiwan at 6.0% were comparatively higher than the rest.

■ Malware Network Activity

Next, we will take a look into the malware activity observed by the MITF. Figure 7 shows trends in the total number of malware specimens acquired during the period under study. Figure 8 shows the distribution of the specimen

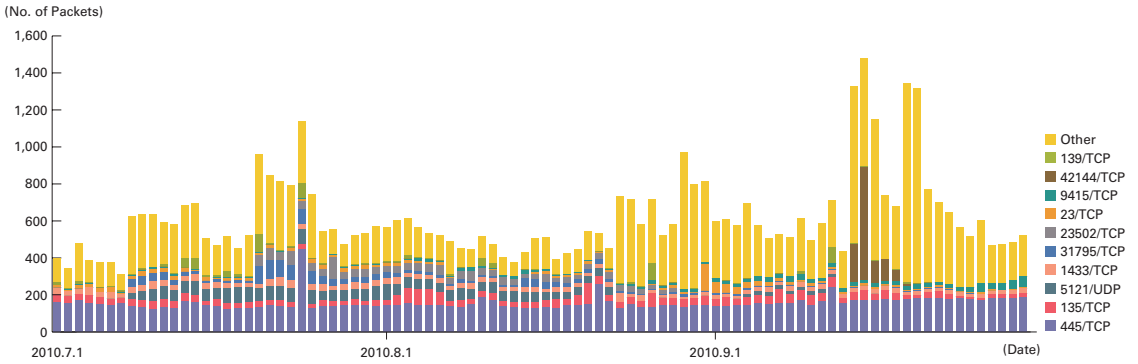


Figure 5: Communications Arriving at Honeypots (by Date, by Target Port, per Honeypot)

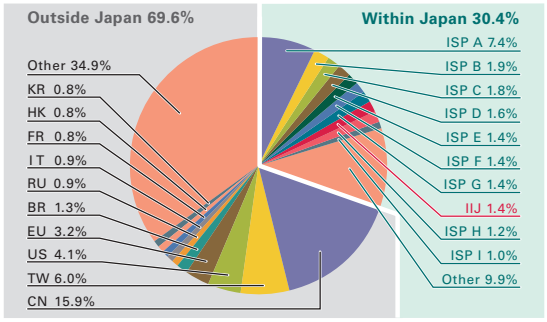


Figure 6: Sender Distribution (by Country, Entire Period under Study)

*33 An abbreviation of Malware Investigation Task Force. The Malware Investigation Task Force (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.

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

acquisition source for malware. In Figure 7, the trends in the number of acquired specimens show the total number of specimens acquired per day*35, while the number of unique specimens is the number of specimen variants categorized according to their digest of a hash function*36.

On average, 371 specimens were acquired per day during the period under study, representing 41 different malware variants. Statistics in our prior report show that the average daily total for acquired specimens was 378, with 32 different variants. During the current period the total number of specimens acquired decreased slightly, but the number of different variants rose compared to the previous period. The sharp drop in total specimens acquired after September 19 is due to the activity of Sdbot and its variants ceasing worldwide. The reason for this suspension of Sdbot activity is not known.

The distribution of specimens according to source country in Figure 8 has Japan at 38.7%, with other countries accounting for the 61.3% balance. Taiwan was at 47.8%, maintaining the large percentage that it held during the previous period. This is due to the high level of activity shown by Sdbot and its variants in Taiwan, but as with other countries this activity ceased after September 19.

The MITF prepares analytical environments for malware, conducting its own analyses of acquired specimens. During the current period under observation 14.0% of the malware specimens acquired were worms, 84.8% were bots, and 1.2% were downloaders. In addition, the MITF confirmed the presence of 26 botnet C&C servers*37 and 276 malware distribution sites. The number of malware distribution sites detected increased dramatically due to the increase in specimens accessing multiple distribution sites, which had dropped in the previous period under study.

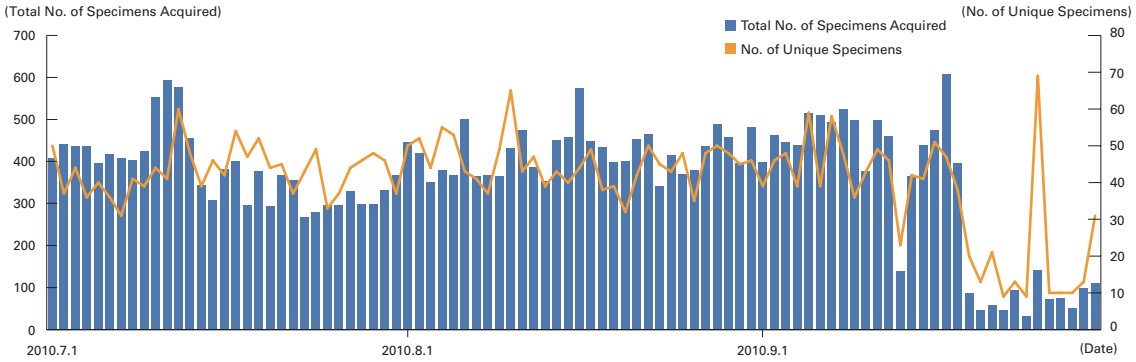


Figure 7: Trends in the Number of Malware Specimens Acquired (Total Number, Number of Unique Specimens)

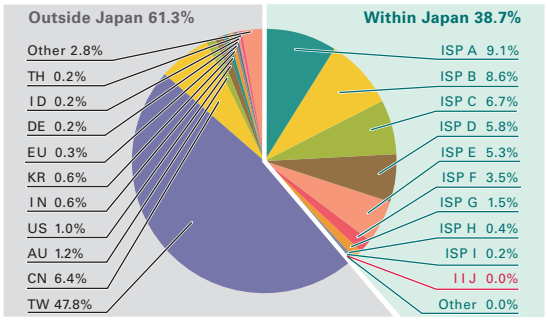


Figure 8: Distribution of Acquired Specimens by Source (by Country, Entire Period under Study)

*35 This indicates the malware acquired by honeypots.

*36 This figure is 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.

*37 An abbreviation of "Command & Control." A server that provides commands to a botnet consisting of a large number of bots.

1.3.3 SQL Injection Attacks

Of the types of different Web server attacks, IIJ conducts ongoing surveys related to SQL injection attacks*38. 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 9 shows trends of the numbers of SQL injection attacks against Web servers detected between July 1 and September 30, 2010. Figure 10 shows the distribution of attacks according to source. These are a summary of attacks detected by signatures on the IIJ Managed IPS Service.

Japan was the source for 40.0% of attacks observed, while China and the United States accounted for 36.7% and 7.1%, respectively, with other countries following in order. There was very little change from the previous period in the status of SQL injection attacks against Web servers. However, as attacks mainly from China against specific targets attempting to gain access privileges on SQL servers occurred on September 30, the percentage of attacks accounted for by China has increased.

As previously shown, attacks of various types were properly detected and dealt with in the course of service. However, attack attempts continue, requiring ongoing attention.

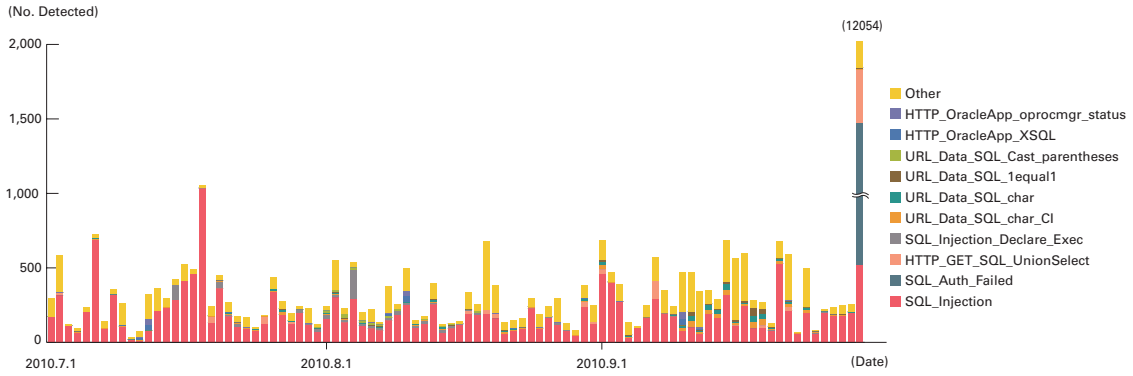


Figure 9: Trends in SQL Injection Attacks (by Day, by Attack Type)

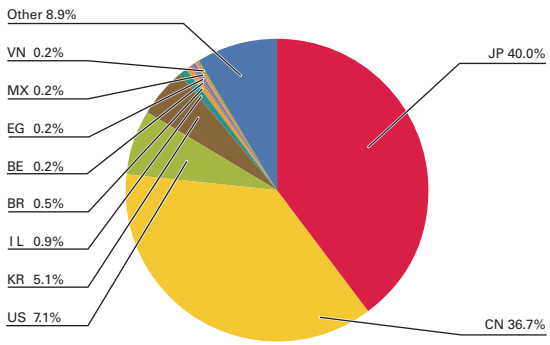


Figure 10: Distribution of SQL Injection Attacks by Source (by Country, Entire Period under Study)

*38 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 continuing to perform independent surveys and analyses. Here we will present information from the surveys we have undertaken during this period regarding preparations to be made for DDoS attacks on small-scale systems and security for shared systems, and also provide an overview of digital forensics.

1.4.1 Preparing for DDoS Attacks on Small-Scale Systems

As shown in "1.3.1 DDoS Attacks," multiple DDoS attacks on Web servers took place during September for the period covered in this report. These attacks targeted the Web servers of both Japanese public agencies and private-sector businesses. DDoS attacks are generally carried out as a form of protest or a personal statement to the owner of the server that is targeted. In recent years there have also been cases in which DDoS attacks are used in blackmail attempts to extort money. Technology such as dedicated attack tools and botnets are used in current DDoS attacks, and some people will even carry out attacks on behalf of others. In other words, those intending to carry out an attack can do so comparatively easily without specialist knowledge or technology. This means there is a chance that any server exposed to the Internet could be the target of a DDoS attack regardless of its scale. Here we examine preparations to be made for DDoS attacks on small-scale systems.

DDoS attacks include those that overload the server itself directly, and those that flood the lines being used by the server with communications. Both of these types of attack cause servers connected to the Internet to be suddenly rendered inoperative. When evaluating countermeasures that will be effective when such an attack occurs, it is necessary to make preparations such as establishing a countermeasure policy based on the server's level of importance, improving the server's tolerance, building a system for abnormal behavior detection, and requesting the cooperation of other organizations.

■ Establishing a Countermeasure Policy

Servers targeted by a DDoS attack will no longer be able to carry out their intended role, which is a threat to availability. Consequently, you should first clarify how business would be affected if a server under examination was to suspend its operations. Once this is done, a target should be set for recovery of server functionality. For example, it is necessary to consider factors such as whether a complete suspension would be problematic for the business, whether it is possible to limit the scope of communications to a certain domain (such as within Japan or business partners only), and whether the quality of communications can be lowered (limiting connections from a certain address or applying bandwidth control across the board). Look into introducing a dedicated DDoS countermeasure device or using a countermeasure service for servers that require high availability.

■ Improving Server Tolerance

Communication lines may become flooded and servers overloaded when you are targeted by a DDoS attack. This means it may be difficult to confirm the communications or operating status of unprotected servers. When installing servers, it is necessary to evaluate the processing ability required for normal business operations and incorporate

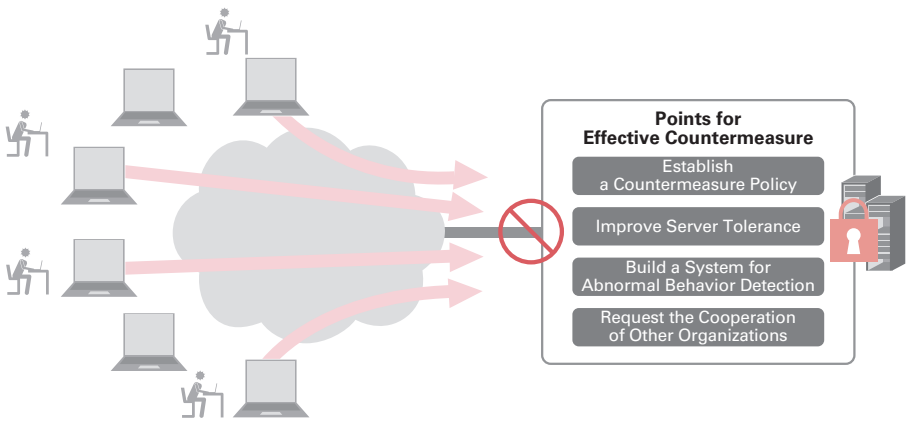


Figure 11: Preparing for DDoS Attacks

a certain surplus over and above this. It is also important to look into implementing DDoS countermeasures and resource management options for the server's OS and applications. For example, Linux incorporates the SYN cookies function*39 that protects against SYN flood attacks, and a function that limits connections for each application*40. Apache HTTP servers also offer functions for limiting elements such as simultaneous connections in their settings*41 or by adding external modules*42. By combining hardware performance with OS and application functions such as these, it is possible to increase a server's tolerance of DDoS attacks.

■ Building a System for Abnormal Behavior Detection

When trying to ascertain the situation after being targeted by a DDoS attack, it can take an extremely long time to complete analysis due to suitable logs not being acquired on a daily basis or the large volume of log data that must be processed. Consequently, it is crucial to record logs appropriately and confirm communications status on a regular basis to prepare a system that detects DDoS attacks as an abnormality. In addition to server logs, referring to data regarding communications from SNMP or Netflow will make it easier to grasp the situation. It is also necessary to prepare for handling logs containing large volumes of data. For example, by setting up a log server separate to the Web servers it is possible to analyze records even when the Web servers are overloaded. Additionally, by preparing scripts for extracting a summary of large logs in advance, it is possible to understand the situation swiftly when abnormal behavior is detected.

■ Requesting the Cooperation of Other Organizations

Sometimes it may not be possible for a targeted server to deal with attacks that flood lines with communications or spoofed IP addresses. In such cases it may be necessary to request help from external organizations such as ISPs, security vendors, or CSIRTs. When doing this you will need to disclose what you have already learned about the situation. Additionally, in many cases the organization from which help is requested will not be able to deal with the threat alone, and it will be necessary to give permission for them to share information about the attack with other organizations (such as the attacker's ISP). By determining the attack information that can be disclosed in advance, such as IP address, attack details, and communication patterns, it will be possible for other organizations to implement countermeasures swiftly. Documents such as the JPCERT/CC incident report form*43 serve as useful reference points for this kind of information.

■ Summary

In this section we have covered a number of points that should be prepared in advance for small-scale systems that may be targeted by DDoS attacks. As shown in the backscatter observations in "1.3.1 DDoS Attacks," DDoS attacks on servers not providing Web content have been observed, and there is a need to prepare for sudden DDoS attacks on all kinds of servers. DDoS attacks embody a strong message from the attacker, and their occurrence can be anticipated to a certain extent. For this reason, paying attention to world trends and news related to your company such as information regarding organizations you belong to and identifying the precursors to conflict at an early stage can serve as helpful preparations against DDoS attacks*44.

1.4.2 Shared System Security

Recently, the full-scale use of cloud computing has begun to accelerate. The cloud makes it possible to use a variety of system resources at low cost by sharing them, but the unique security issues faced by shared systems are of concern. Here we examine the threats that occur in the cloud due to shared system resources as well as their countermeasures.

*39 See Daniel J. Bernstein's explanation of SYN cookies (http://cr.yp.to/syncookies.html) for more details. IETF's RFC4987 "TCP SYN Flooding Attacks and Common Mitigations" (http://www.ietf.org/rfc/rfc4987.txt) also provides a summary covering the principles behind SYN flood attacks as well as countermeasure technologies.

*40 iptables provides modules such as limit and connlimit. For example, using the iptables limit module to limit syn packets makes it possible to set a cap on the number of new connections that an application can process.

*41 It is possible to use the MaxClients setting to limit the number of simultaneous connections. You can also contain the resources consumed by an attack by adjusting settings such as Timeout, KeepAlive, KeepAliveTimeout, and MaxKeepAliveRequests.

*42 A large number of external modules exist for Apache. One example, mod_limitipconn (http://dominia.org/djao/limitipconn2.html) makes it possible to limit the number of simultaneous connections from a single IP address.

*43 See the following JPCERT Coordination Center page on incident reporting for more details (http://www.jpcert.or.jp/english/ir/form.html).

*44 Other useful information on DDoS attacks includes VeriSign Inc.'s "DDoS Mitigation – Best Practices for a Rapidly Changing Threat Landscape Whitepaper" (user registration required) (http://www.verisign.com/forms/ddosbestpracticeswp.html?toc=MYUM9-0000-02-00).

Issues with Shared Resources

System resources are shared in a multi-tenant cloud, with the partitioning of resources between users handled logically by software, etc. For this reason it is crucial this logical resource partitioning is handled appropriately, as breaking the boundaries of a partition would represent a security threat for users. Let us examine the potential threats that could actually occur. The CSA (Cloud Security Alliance)*45 lists seven items as threats to cloud computing in "Top Threats to Cloud Computing V1.0"*46. These include "Shared Technology Issues," which covers incidents and impact from the improper logical partitioning of shared resources such as CPU and GPU. Shared resources have also been brought up as a threat unique to cloud computing in many articles other than the CSA report. As resources such as communication lines, communication devices, and storage are also shared in the cloud, these must also be considered. Here we look at concrete examples of threats while considering cloud system architecture.

Architecture of Cloud Infrastructure

The architecture of a cloud is generally not made public. For this reason, we assume a cloud composed of generic equipment, and use a cloud system comprised of the devices shown in Figure 12 as an example to evaluate threats to cloud computing.

This cloud uses a router or similar device to connect to the Internet. Users access VM (virtual machines) on the cloud via the Internet (the red arrow in Figure 12). The physical machines running these virtual machines also accommodate the virtual machines of other users, so the physical resources are shared. The physical machines have multiple Ethernet ports for providing service, including those for connecting to the Internet and those providing storage services via an Ethernet connection to a storage network (IP-SAN).

Users access VMs using the route shown by the red line in the figure. Users are generally not aware that they are working on a complex device layout when using the cloud. A shared environment that is not visible to its users may have inherent security issues.

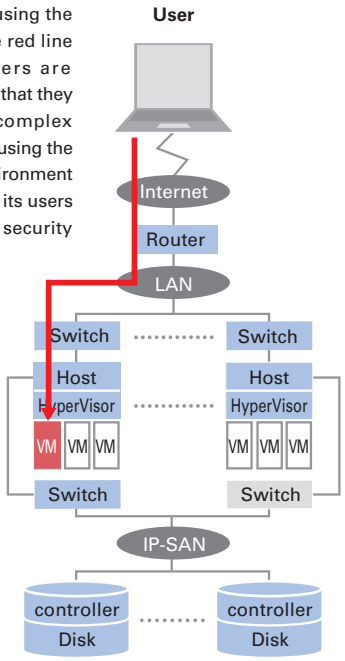


Figure 12: Sample Cloud System Architecture

Cloud Environment Threats and their Countermeasures

Sharing network resources is not unique to cloud environments, as the Internet itself and rental server environments also involve multiple users sharing a network. However, in this sample cloud there is the possibility that virtual machines with different security policies will occupy that same L2 segment. A virtual machine could be hacked and hijacked, presenting the risk of communications being blocked or intercepted via methods such as ARP poisoning*47. To counter threats such as these it is necessary to implement measures for preventing the spoofing of the VLAN ID or MAC address in hypervisor or the connected switch.

In this sample cloud, storage is also shared through virtualization. When technology such as IP-SAN (iSCSI) is used, storage is connected via Ethernet, making it possible to attack a storage network by artificially generating a fake Ethernet frame. When a storage controller exists on a network location reachable by virtual machines, attacks against this controller are also possible. Additionally, when the ID (IQN*48) for storage virtualization is falsified, there is a risk that data areas that should be partitioned and invisible could be

*45 CSA (Cloud Security Alliance) is an organization established in 2008 to promote best practices for cloud security (http://www.cloudsecurityalliance.org/). The Cloud Security Alliance Japan Chapter came into being in June 2010 as the Japan branch of the organization (http://www.cloudsecurityalliance.jp/) (in Japanese).

*46 In "Top Threats to Cloud Computing V1.0," the CSA documents threats that are typical to cloud computing as well as their countermeasures (http://www.cloudsecurityalliance.org/topthreats/csathreats.v1.0.pdf).

*47 ARP poisoning is an attack that involves sending spoofed ARP packets to a network to intercept communications from other hosts.

*48 An abbreviation of "iSCSI Qualified Name." This is the name used to identify iSCSI nodes on a network.

viewed and connected to. To counter threats such as these it is necessary to implement access controls or spoofing countermeasures in hypervisor or the switch in the same way as with network threats.

Additionally, when basic functions such as firewalls are provided as part of a service, threats vary depending on the form in which they are provided. Figure 13 shows sample firewall placements. Pattern 1 represents the method in which a firewall is provided as a hypervisor function. In this case firewall security is guaranteed by the service provider. In pattern 2 a software firewall solution is applied by installing an OS on the hypervisor in the same way as the virtual machines provided to users. This would mean that when vulnerabilities exist in the hypervisor, the firewall would also be affected. In pattern 3 a dedicated device is prepared and network traffic relayed through it using VLAN and routing. This method replicates existing models, but has a higher cost. In pattern 4 the firewall is implemented on the user's OS, but this presents the risk of settings being changed by hackers. Pattern 5 represents a method often used for the Web and email, in which an application's proxy function is used as SaaS. When services are offered by several different providers, regulation between services is the responsibility of the user. These examples demonstrate the need to be aware that different points must be considered depending on the form of service provided.

■ Summary

The items explained here are not new concepts, and under normal conditions as long as the service provider is aware of each threat and takes appropriate countermeasures, there should be no risk of issues occurring.

It is helpful for users to be aware of internal architecture to confirm security, but in many cases this kind of information is not disclosed when using a service. When using a cloud, it is important for users to assess their scope of responsibility with regard to the services they use and implement the necessary countermeasures, while also reaching agreement regarding security measures with the service provider.

1.4.3 An Overview of Digital Forensics

With the spread of IT much of the information retained by companies and individuals is saved and accumulated as digital data. Because of this, cases in which digital data is used in incident responses or as evidence in trials are on the rise. Digital data is more easily changed or destroyed than physical media, so those who investigate such matters must have access to appropriate technology. Here we will explain the digital forensics techniques that are used to examine digital data.

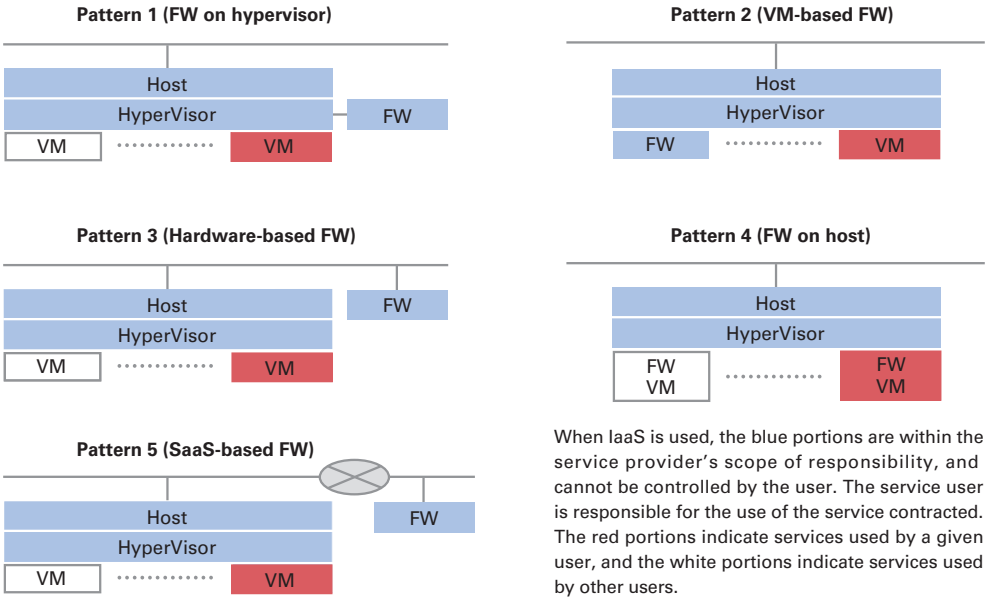


Figure 13: Sample Firewall Placements

Digital forensics is a technology used mostly in corporate environments*49 in situations such as incident responses investigating unauthorized access or when presenting digital data for a trial. To categorize digital forensics from the perspective of the subject matter being analyzed, it includes computer forensics for analyzing computers, network forensics*50 for analyzing packets sent over a network, and mobile device forensics*51 for analyzing mobile devices such as mobile phones.

Digital forensics is carried out by acquiring, analyzing, and reporting data in that order. Apart from certain exceptions, digital forensics is generally not carried out by using the original digital data for analysis. Engineers carrying out digital forensics first acquire the data in question. Next, the acquired data is analyzed using appropriate tools, and the series of events related to the incident are reconstructed. Last of all, the established facts are put together in a report based on the results of the analysis.

■ Computer Forensics

Next, we will cover the acquisition and analysis process for computer forensics, which is frequently used.

Computers are comprised of components such as the CPU, memory, and hard disks. Data on hard disks or CD-ROM media is non-volatile and remains intact even when the computer is powered down. Data in the CPU and memory is volatile, and is lost when the power is turned off. In RFC3227 "Guidelines for Evidence Collection and Archiving"*52 it is recommended that when acquiring data you should proceed from the volatile to the less volatile. Accordingly, when the computer being examined is a server in an online state (powered on and running), it is best to first collect volatile data such as that found in memory before collecting data on the hard disk or other backup media.

Methods for collecting volatile data include executing a volatile data gathering toolkit on the machine in question, and acquiring a memory image for later analysis. An example of a volatile data collection toolkit is Sysinternals Suite*53.

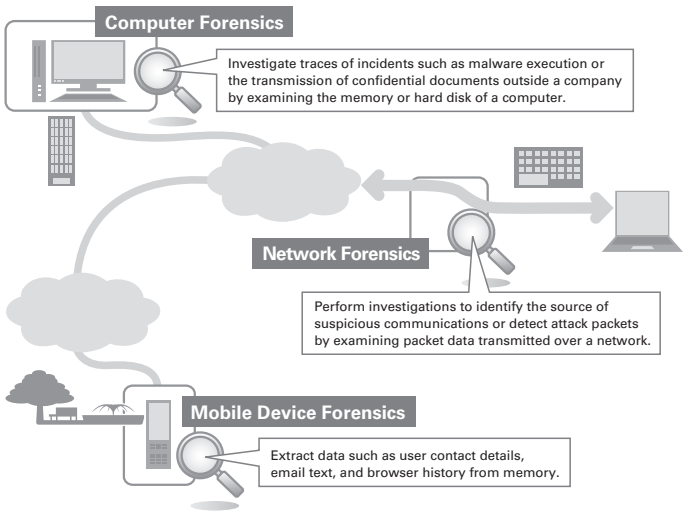


Figure 14: Forensics Overview

*49 NPO The Institute of Digital Forensics defines digital forensics as "a series of scientific investigation methods and technologies for acquiring evidence, investigating, and analyzing electromagnetic records for incident response and legal disputes/litigation, and the analysis and data collection related to the alteration or damage of electromagnetic records." (http://www.digitalforensic.jp/wdfitm/wdf.html) (in Japanese).

*50 Techniques for investigating and analyzing computers remotely are also sometimes referred to as network forensics.

*51 Mobile device forensics was seldom implemented outside law enforcement agencies in Japan because the forensic tools used in Europe and America do not support Japanese mobile phone specifications. However, tools compatible with the smartphones that are growing in popularity recently have started to become available for use in Japan. For example, Oxygen Software's Oxygen Forensic Suite tool for mobile device analysis is now used by the Cyber Defense Institute Inc. (http://www.cyberdefense.jp/company_profile/prerelse10001.html) (in Japanese).

*52 RFC3227 "Guidelines for Evidence Collection and Archiving" (http://www.ietf.org/rfc/rfc3227.txt) contains evidence collection procedures and cautionary notes for when a security incident occurs.

*53 Sysinternals Suite includes a wide variety of programs, such as PsList for showing information about the processes being executed and TcpView for showing TCP connection status (http://technet.microsoft.com/en-us/sysinternals/bb842062.aspx).

This group of tools is executed on the target machine, with results output as a text file or similar format. Meanwhile, a memory image refers to a raw dump of the contents of memory in binary file format. To acquire a memory image a tool is executed on the target machine to dump the memory, and this memory image is later transferred to another machine for analysis to extract the volatile information. Memory images must always be acquired before executing a volatile data collection toolkit*54.

Methods for acquiring non-volatile data include online and offline acquisition (with the computer in a powered down state). Data may be saved as physical disk images for acquiring each physical disk, or as logical disk images for acquiring each logical volume. In general, non-volatile data is acquired offline. However, when it is more convenient to acquire data as logical volumes, such as when disks are encrypted or in a RAID configuration, acquisition may also be carried out online. A hash value is calculated for the acquired data at the time of acquisition to ensure the integrity of the data after it is acquired. This makes it possible to detect whether data has been changed or falsified after acquisition.

By analyzing acquired volatile data it is possible to obtain information such as the user that was logged in, the communications status and start times of the running processes, the files and shared libraries accessed by processes, the ARP table, the routing table, and the DNS cache. It may also be possible to acquire information such as processes previously executed and communications that had already been closed by analyzing memory image files.

A broad array of results can be acquired through analysis of non-volatile data. Because related executable files and logs are often deleted during a hacking or malware infection incident to conceal the attack, deleted files are recovered and log fragments from unallocated disk space examined. Furthermore, if it is possible to detect operations or files related to an incident from system and event logs or the registry, you can estimate the time an incident occurred and the scope of damages by examining other events close to the time the operations were carried out or the time stamp (data indicating the time a file was created or updated) of corresponding files.

Also, by searching for keywords in acquired data, whether volatile or non-volatile, it is possible to confirm traces of data communications to external parties, and check whether other systems have been accessed*55.

Issues with Digital Forensics

The following issues are present in digital forensics.

- Consolidating logs from multiple sources
- Dealing with anti-forensics
- Dealing with large volumes of media and encryption

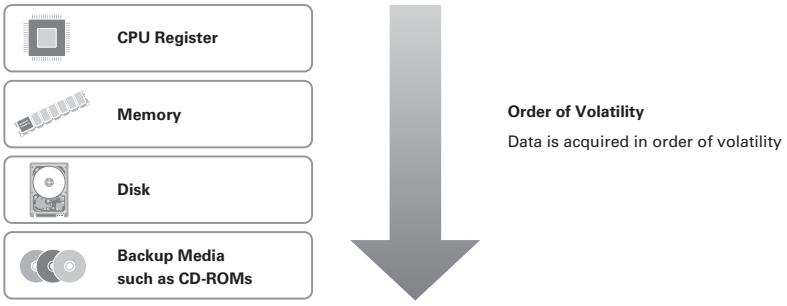


Figure 15: Order of Volatility

*54 A volatile data collection toolkit is composed of a large number of programs that may influence the content of a memory image due to actions such as a swap occurring when they are executed.

*55 Examples of the tools for conducting data analysis indicated here include EnCase (http://www.guidancesoftware.com/), FTK (http://www.accessdata.com/), and TSK (http://www.sleuthkit.org/).

An example of a case affected by the issues with consolidating logs from multiple sources is the examination of the extent that confidential information has spread in an information leak. When conducting such an examination, network forensics must be carried out in addition to computer forensics. Specifically, it is necessary to compare the logs and packet data from network devices such as firewalls, routers, and IDS with the data from the computer. However, when the logs for each device have different formats or time settings this comparison work becomes an enormous task.

Anti-forensics are techniques for evading detection by digital forensics. For example, to evade techniques that examine related files based on file system time stamps, some malware sets a random time in the time data of files it creates. To deal with this kind of anti-forensics, it is necessary to utilize time stamps other than those set on the file system*56.

The size of media to be acquired is also growing year-on-year. To acquire data in the shortest time possible the only option is to make improvements to the performance of acquiring devices and software. However, when there is not enough time, one technique that can be utilized is previewing data before it is acquired (examining the given media directly by mounting it with read-only access). It would also be desirable to automate processes to analyze large volumes of media in an efficient manner. There have recently been many cases in which the target media has been encrypted. In this case it is necessary to either acquire data online, or decrypt the data once it has been acquired offline.

Summary

Using digital forensics in incident responses makes it possible to examine the cause of an incident as well as the extent of its impact without overlooking any key data. IIJ will continue to look into ways of resolving the issues faced by digital forensics while constantly evaluating the latest technology trends and applying these findings to our response methods.

1.5 Conclusion

This report has provided a summary of security incidents to which IIJ has responded. In this report we examined the preparations necessary for incident response by looking at preparations to be made for DDoS attacks on small-scale systems and security for shared systems such as a cloud computing, as well as giving an overview of digital forensics.

By identifying and publicizing incidents and associated responses in reports 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 secure use of the Internet.

Authors:
Mamoru Saito
Manager of the Office of Emergency Response and Clearinghouse for Security Information, IIJ Service Division. 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, the Web Malware Mitigate Community, and others. He is also active in organizations such as the Engineers SWG of the Anti-Child Pornography WG in the Association for Promoting the Creation of a Safe Internet, and the IPA Conference for Denial of Service Attack Countermeasures.

Hirohide Tsuchiya (1.2 Incident Summary)
Hirohide Tsuchiya, Hiroshi Suzuki, Tadaaki Nagao (1.3 Incident Survey)
Mamoru Saito, Hirohide Tsuchiya (1.4.1 Preparing for DDoS Attacks on Small-Scale Systems)
Masahiko Kato (1.4.2 Shared System Security)
Takahiro Haruyama (1.4.3 An Overview of Digital Forensics)
Office of Emergency Response and Clearinghouse for Security Information, IIJ Service Division

Contributors:
Yuji Suga, Hiroaki Yoshikawa, Tadashi Kobayashi, Seigo Saito
Office of Emergency Response and Clearinghouse for Security Information, IIJ Service Division

*56 Examples of other time stamps include data recorded within files, the data for an original file found in a shortcut file, and registry key information. For malware infections made through Web browsers or emails, browser history and the times email has been sent or received can also be of help.

Steps Towards Implementing DNSSEC

The Domain Name System is an essential part of the Internet. Here, we look back on the role of DNS, and examine the challenges and future prospects for the implementation of the DNSSEC technology that responds to the threats to DNS that are of concern today.

2.1 The Role of DNS

DNS is a service that simply returns resource records in response to queries, but this service is indispensible for the operation of the Internet. For example, though users themselves are seldom aware of this, everyday Internet usage such as the viewing of pages on a Web browser or the sending and receiving of email rely on DNS behind the scenes. Of course, DNS is not required for communications. However, due to factors such as the need to remember the IP address of the other party, the usefulness of the Internet is greatly hampered without DNS, and it is realistic to say that many users are dependent on it.

DNS enables the distributed management of the Internet, dividing it into areas known as zones. The top level of the Internet is the root zone, which is represented by a period (“.”). By setting subdomains as needed and delegating their administration, a tree-like hierarchy of distributed management is formed. For example, the .jp country code top-level domain is administered by Japan Registry Services Co., Ltd., and all registered .jp domains are published through a group of content DNS servers called JPDNS. When queries are made, the required resource records are located via this tree-like hierarchy of content DNS servers that are delegated to other organizations and managed in a distributed manner.

In many cases the user’s terminal does not handle this process itself, but rather sends a query to a cache DNS server operated by an ISP or network administrator. The cache DNS server responds to the terminal’s query by locating the content DNS server, searching for the required resource records, and returning the results to the terminal. If DNS is not operating correctly, it results in the target service being rendered inaccessible. Incidents of websites not being accessible due to problems with DNS actually occur quite often worldwide.

2.2 The Need for DNSSEC

The most insidious problem with the operation of DNS servers is false responses. When an incorrect resource record is sent back in response, the party receiving this response is likely to trust this information, and due to the mistaken details a great deal of trouble can be caused. As some people have harmful intentions, attacks that inject these false responses intentionally have been known to occur. When these attacks succeed, it is possible to lead users attempting to access certain websites to completely unrelated sites of the attacker’s choosing. It is easy to imagine

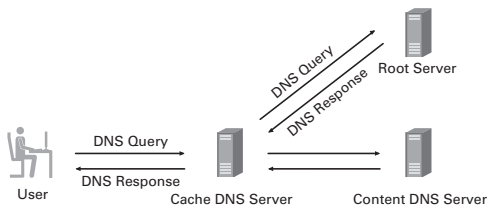


Figure 1: DNS Queries and Responses

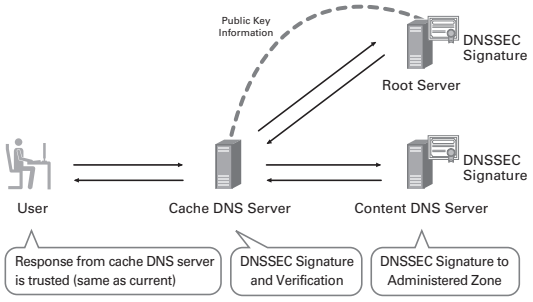


Figure 2: DNSSEC Implementation

how this could result in problems such as the stealing of account information. To make matters worse, these attacks are possible using the terminals and Internet speeds available today.

With these kinds of attacks in mind, related parties have been evaluating the implementation of a technology called DNSSEC, which makes it possible to verify whether or not a DNS response is legitimate. DNSSEC authenticates the sender of a response by attaching a digital signature that uses a public key encryption method to DNS responses, making it possible to confirm the integrity of a response.

Under DNSSEC, digital signatures are created for each zone. Public key information is required to verify these signatures. With DNSSEC, it is possible to register the public key information used in signatures on a subdomain to a zone as a resource record. By doing this, when the public key information for a certain zone is acquired, it is possible to carry out verification for its subdomains by following the registered public key information. This chain of trust makes it possible to verify DNSSEC from any given zone, and as long as the chain of trust is not broken and the root (.) public key information is acquired, all signed zones can be verified.

2.3 Work Towards Support for DNSSEC

When considering support for DNSSEC as the administrator of a zone, two tasks are required. The first is the signing of the zone, and the second is the registration of the public key information used with the signature to the higher level zone. The signing of a zone is closely related to key operation, and requires knowledge of public key encryption and ongoing updates and signing of keys. Additionally, when public key information is registered to the higher level zone, the registry administering that zone and the registrar serving as the point of registration must also of course support DNSSEC. The .jp country code top-level domain began DNSSEC signatures for the JP zone on October 17, 2010. Registry support, meaning the start of acceptance of public key information registration, is scheduled for January 16, 2011.

On the query-handling side, it is thought that the model to be adopted will involve DNSSEC verification first being carried on a cache DNS server operated by an ISP or network administrator, with terminals trusting these verification results. The cache DNS servers that carry out this DNSSEC verification must acquire the public key information to serve as the basis of trust for the domain to be verified. With the root (.) zone now DNSSEC signed, setting the root zone's public key information would be a straightforward method of operation, but depending on operating policies it should also be possible to limit verification to the required area only. In either case, this public key information must be updated in conformance with the timing of updates to the key itself.

There have actually already been many reports of problems relating to the operation of DNSSEC. These range from simple cases in which updates were neglected to those in which there were issues with the operation tools. When problems with DNSSEC occur, in most cases the signature verification process will fail, and the cache DNS server will return an error. This means that the user will not receive the required response from the DNS. In actual fact, the problems mentioned above had a significant impact on operations, with many users not able to access websites. Though the goal of implementing DNSSEC is to improve security, if it cannot be operated properly, it causes issues such as rendering sites inaccessible.

DNSSEC requires knowledge of public key encryption and ongoing update work, and demands stricter operation of DNS than before. Unfortunately, this means that at present it is not something that can be implemented easily. Despite this fact, a function that enables verification of DNS responses is of great importance, and for services that may face considerable damages when a DNS response is forged, it is worth considering creating an operating framework and implementing this technology. IIJ has carried out a various trials and surveys working towards the implementation of DNSSEC. We have also actively cooperated in the implementation of DNSSEC on a number of top-level domains. We hope to put the knowledge we have gained to use in providing a safer Internet environment through DNSSEC.

Author:
Yoshinobu Matsuzaki
Mr. Matsuzaki is a Senior Engineer in the Technology Promotion Section of the Network Service Division in the IIJ Network Service Department. Mr. Matsuzaki is always finding things that pique his interest while striving at his work. He is an IIJ-SECT member, co-chair of The Asia Pacific OperatorS Forum, chair of APNIC IPv6 SIG, and an expert advisor for JPCERT/CC.

Sender Implementation of Sender Authentication Technology Sluggish

In this report, we will present an overview of spam trends for week 26 through week 38 of 2010. The United States replaced China as the top regional source of spam. We also discuss the implementation status of sender authentication technology and botnet countermeasures.

3.1 Introduction

This report summarizes the latest trends in spam, covers email-related technologies, and touches on various other activities in which IIJ is engaged.

In this volume we focus on data for the second quarter of 2010, representing the period of 13 weeks from week 26 (June 28 to July 4) to week 38 (September 20 to September 26).

3.2 Spam Trends

In this section, we will report on historical ratios of spam and the results of our analysis concerning spam sources based on trends detected by the Spam Mail Filter provided through IIJ's email services.

3.2.1 No Increase in Spam in September unlike Previous Years

The ratio of spam averaged 79.0% of all incoming emails over the 91-day period from week 26 to week 38, 2010. This compares to an average of 81.3% for our last survey (week 13 through week 25, 2010), and 82.2% for the same period in 2009 (week 27 through week 39), indicating a slight decrease for both. Figure 1 shows spam ratio trends from week 27 of 2009 onward, including the results for the current period.

Trends in surveys for the previous years showed a drop in regular email volume during week 32 (August 9 to August 15), which coincides with a holiday period in Japan, and this caused the ratio of spam to increase. Although the spam ratio subsequently declined, it would rise again in September. During the current survey period the ratio followed a similar pattern up to August, with week 32 showing the highest ratio of spam at 82.6%. However, the ratio stayed low in September, and the overall average spam ratio for the period was lower than in previous years. It is not clear if this is a temporary decline, or if for some reason the decreased spam volume will be sustained in the future. We will continue our analysis and surveys of the situation.

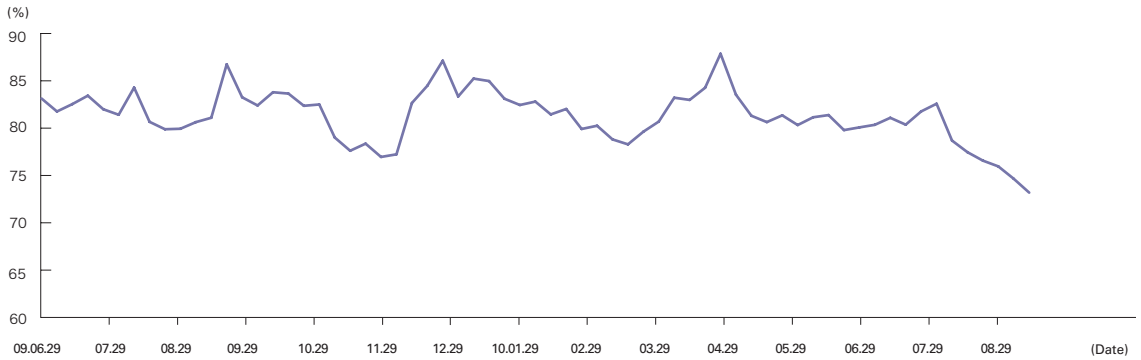


Figure 1: Spam Ratio Trends

3.2.2 The United States Replaces China as the No. 1 Regional Source of Spam

Figure 2 shows our analysis of regional sources of spam over the period studied. The United States (US) was the number one source of spam in this survey, accounting for 11.3% of total spam. It rose from 2nd place in the previous survey to take the top place once more. India (IN) was 2nd at 7.4%, rising from 3rd place in the previous survey. China (CN), which took the top position in the previous survey, was 3rd this time at 7.1%. Additionally, Great Britain (GB) and Germany (DE), which demonstrated upward momentum in the previous survey, maintained high rankings at 5th (5.0%) and 7th (4%), respectively. Other regions that have held high ratios previously remained in the upper rankings, with Brazil (BR) at 4th (5.2%) and Vietnam (VN) at 6th (4.8%). Japan (JP) dropped to 8th, with its ratio falling 0.1% to 3.8%.

Figure 3 shows trends in ratios for the six main regional sources of spam (US, IN, CN, BR, GB, and VN). Though the ratio for previous top place holder China (CN) dropped in July, it began to rise again in August, and there is a chance it will once again become the top regional source of spam in the future. Current 1st place holder the United States (US) had the top ratio for almost the entire period under study, and was highest overall. There were no significant changes for the other 4 top regions (IN, BR, GB, and VN). However, current 2nd place holder India (IN) fluctuated between 1st and 2nd position, and I believe we must continue to keep a close eye on the situation there.

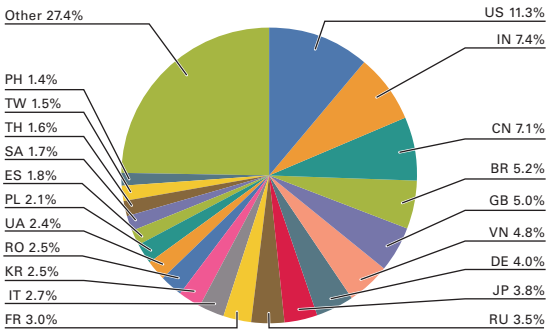


Figure 2: Regional Sources of Spam

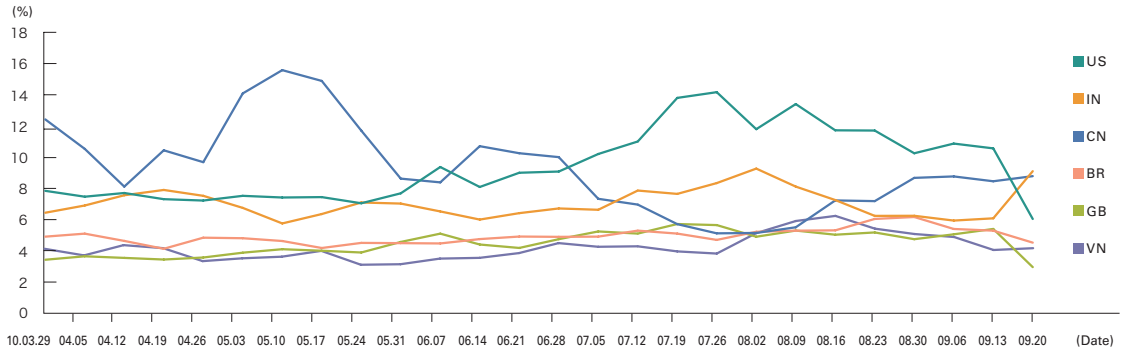


Figure 3: Trends in the Top 6 Regional Sources of Spam

3.3 Trends in Email Technologies

In this section we continue to report on the implementation status of the SPF (Sender Policy Framework) sender authentication technology that has become widely prevalent. We also look at examples of initiatives for eradicating botnets, which play a major role in the sending of spam.

3.3.1 Sender Authentication Technology

Sender authentication is generally carried out as standard for email received via the email services that IIJ provides. Figure 4 shows the ratios for authentication results during the current survey period (July to September, 2010). Of the emails received during this period, 55.7% indicated "none" as the authentication result. This means that the domain for approximately 44.3% of email received declared an SPF record. This is a 0.8% drop compared to results for the previous period. This ratio also dropped in survey results for the JP domain only (Figure 5). The WIDE Project survey*1 also indicated marginal change from the previous period, so we can surmise that domains implementing this technology have not increased significantly.

The Ministry of Internal Affairs and Communications has published statistical data regarding trends in SPF authentication ratio for 6 telecommunications carriers including IIJ since August, 2009*2. The latest data for August 2010 showed authentication results indicating "none" at approximately 18%, meaning that the domain for approximately 82% of email received declared an SPF record.

This result differs greatly from those found in this report. It is thought that this discrepancy arises from differences in the email service user base and aggregation points. For example, the majority of email received on mobile phones is sent from other mobile phones. Most domains for mobile telecommunications carriers declare an SPF record, so we can expect high ratios for this in the authentication results. This means that to ascertain the trends for implementation of sender authentication technology, it would be better to make conclusions based on changes over time for each ratio rather than comparing absolute values for each piece of data. Implementation ratios were already high at the point that data aggregation began, so for both sets of results we can see that the trends indicate implementation is still not progressing.

3.3.2 Botnet Countermeasures

Germany (DE), which was the 7th highest regional source of spam in this report, launched the German Anti-Botnet Initiative*3 in September of this year to eradicate botnets, which are a popular mechanism for sending spam. This is a project jointly operated by the German Internet industry association "eco" and the Federal Office for Information Security (BSI). Through this initiative warnings are sent to users infected by malicious software, and their Internet access is also restricted until the infection is removed. The aim of the project is to help users clean their PCs by providing support such as tools for removing malicious software and a telephone help desk. This may appear very

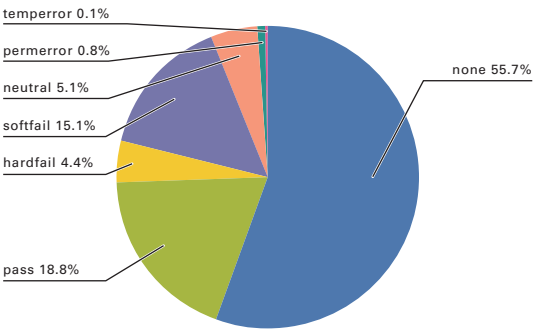


Figure 4: Sender Authentication Result Ratios

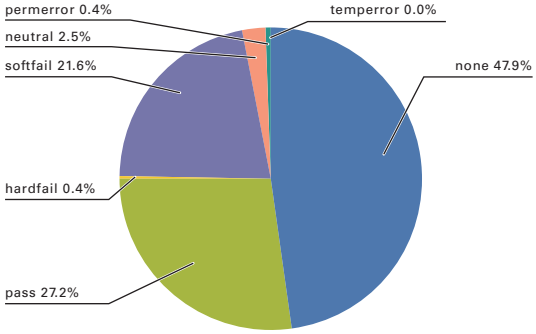


Figure 5: Sender Authentication Result Ratios (JP Domains Only)

*1 Approximate deployment ratios for JP domain authentication technology as of August 2010 (http://member.wide.ad.jp/wg/antispam/stats/).
*2 http://www.soumu.go.jp/main_sosiki/joho_tsusin/d_syohi/m_mail.html#toukei (in Japanese)
*3 http://www.oecd.org/dataoecd/42/50/45509383.pdf

similar to the initiatives of Japan's CCC (Cyber Clean Center)*4. In actual fact, members of the eco association involved in this project have held hearings and other meetings with CCC participants, and I believe they have applied many aspects of CCC initiatives to their own. The activities of the CCC were also reported on at the MAAWG General Meeting held in June of this year.

When the goal is simply to stop the sending of spam, the OP25B (Outbound Port 25 Blocking) method deployed widely throughout Japan is extremely effective at preventing the direct sending of email from dynamic IP addresses. In addition to the sending of spam, botnets are also used for more serious Internet crimes such as the distribution of malicious software, DDoS attacks, and the exploitation of personal information stored with a PC. Consequently, it is first necessary for telecommunications carriers to implement OP25B to suppress the circulation of spam containing malicious software in attachments, which serves as the primary cause of botnet creation. Infected PCs are then identified using data such as the details of blocked email and DNS queries that malicious software use to receive commands. It is also possible to use honeypot to detect the source of unauthorized access attempts. Then, similarly to the CCC and German Anti-Botnet Initiative activities, removal tools are distributed to remove the malicious software that form botnets.

As demonstrated here, a procedure for eradicating botnets has been established to a certain extent. However, the removal of malicious software involves considerable cost. The cost of the projects in Japan and Germany are born mostly by the government (for the first year in the case of Germany), but ultimately it is the citizens of each country that foot the bill. To reduce this burden it is crucial that individual users maintain vigilance and prevent their PCs from being incorporated into a botnet.

3.4 Conclusion

The Act on Regulation of Transmission of Specified Electronic Mail, which could be considered Japan's anti-spam legislation, incorporates a provision that it be revised three years after it comes into effect. The act was issued in 2002 and amended in both 2005 and 2008, and from September of this year meetings have been held to discuss the anti-spam measures that will be required in the future in light of the act's current enforcement status. An Unsolicited Mail Measure Working Group was established under the Research Group for ICT Service Issues from a User's Perspective, and discussions took place at the meetings of this working group*5. IIJ continues to participate in discussions regarding the revision of the Act on Regulation of Transmission of Specified Electronic Mail, and the author of this report is a member of the working group in question.

The previous amendment introduced drastic changes with an opt-in regulation that makes prior consent necessary when sending specified electronic mail (in other words, email advertising a product or service). However, looking at the email I have received personally, spam advertising various products and services that I have no recollection of opting in for continues to arrive in my inbox. There are many reasons behind the continued prevalence of spam, but I think one of the primary factors is the fact that it is impossible to determine the sender of such email.

I believe the popularization of sender authentication technology will go some way towards resolving this issue. IIJ will continue to actively participate in anti-spam measures, including the legal aspects presented here, while also working towards resolving technological issues.

Author:
Shuji Sakuraba
Mr. Sakuraba is a Senior Engineer in the Application Service Department of the IIJ Service Division. He is engaged in the research and development of messaging systems. He is also 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, as well as chief examiner for the Sender Authentication Technology Workgroup. He is also a member of Internet Association Japan's Anti-Spam Measures Committee. He is a member of the Ministry of Internal Affairs and Communications' Unsolicited Mail Measure Working Group.

*4 http://www.ccc.go.jp/en_index.html
*5 http://www.soumu.go.jp/menu_sosiki/kenkyu/11454.html (in Japanese)

A Report on Proof-of-Concept Tests for our Next-Generation Modular Eco-Data Center

In February 2010, IIJ began conducting year-long proof-of-concept tests in central Japan using an outside-air-cooled container unit as part of plans to construct a next-generation modular eco-data center. Here we discuss the goals of these proof-of-concept tests, the system configuration used for testing, and the results that have been obtained so far.

4.1 Reasons for Decision to Carry Out Proof-of-Concept Tests using an Outside-Air-Cooling System

4.1.1 The Need to Re-Examine Cooling Systems

Data centers are fitted with high-capacity electrical and cooling equipment to create an environment that facilitates the efficient installation of IT equipment such as large numbers of servers. However, existing data centers now face the problem that servers are emitting far more heat than expected at the design stage, making sufficient cooling impossible. This is due to advancements in the processing power and density of IT equipment, leading to an increase in the power consumed and heat generated by each device. When designing the facilities the effective power consumption for each of the server racks in existing data centers was estimated to be approximately 1 to 3kVA, but this is now commonly 4 to 6kVA, and in the future may rise to 10kVA or more.

Additionally, to fulfill the international commitment to reduce 2020 greenhouse gas emissions to 25% below 1990 levels, and our obligation to reduce total CO_2 levels due to the Tokyo Metropolitan Ordinance on Environmental Preservation, steps must be taken to reduce the power consumption of our data centers.

IT equipment consumes the most power in a data center. However, cooling equipment also consumes a similar amount of power. This means that to make substantial reductions in power consumption it is necessary to review existing cooling systems and introduce new systems that consume less power.

Cooling systems for reducing power consumption include the following two systems, which make use of the outside environment. The term “free cooling” is often used to indicate systems with water-side economizers (chiller-less water cooling systems), but systems with air-side economizers (outside-air cooling systems) fall under the category of free cooling as well, as they also offer reduced power consumption.

- Water-side economizer (chiller-less water cooling systems)
- Air-side economizer (outside-air cooling systems)

As shown in Figure 1, chiller-less water cooling systems use cooling towers that make use of the vaporization heat of water to produce cooling water with less power. On the other hand, outside-air cooling systems make use of cold outside air to cool data centers.

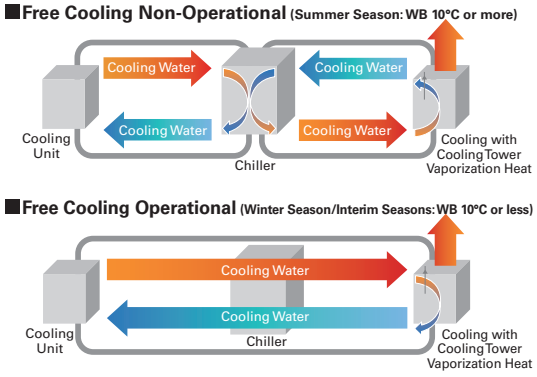


Figure 1: The Principles of Chiller-less Water Cooling Systems

Table 1: Free Cooling System Comparison

	Water-side economizer chiller-less water cooling systems	Air-side economizer outside-air cooling systems
Mechanism	Indirect cooling of interior using cooling water cooled utilizing water vaporization heat (cooling towers)	Direct cooling of interior using outside air
Humidity and Dust Particle Management	Basic humidifiers and filters can be used because interior air is circulated	Humidifiers and filtering equipment are required because outside air is brought directly inside
Facility Characteristics	Cooling towers and chilled water piping are required	Difficult to implement in existing buildings because openings are required in the server room to admit outside air
Main Running Costs	Supplementary water for cooling tower vaporization, power for pump that circulates cooling water, power for indoor equipment	Power for fans that intake outside air
Hours Usable Each Year	3500 to 4000 hours / 8760 hours (Tokyo)	5500 to 6000 hours / 8760 hours (Tokyo)
Implementation Status in Japan	Numerous	Used mostly during interim seasons, with very few examples designed for winter season use

As shown in Table 1, each of these systems has unique characteristics. Following the results of simulations, IIJ decided that the outside-air cooling system was most suitable for our next-generation data centers due to the longer usable hours per year and the lack of a need for equipment such as cooling towers.

However, outside-air cooling systems require openings to be made in the server room for the intake and exhaust of large volumes of air. This posed a large problem that could not easily be resolved when introducing outside-air cooling systems into existing buildings. As a result, IIJ decided to develop container modules that also integrated ducts and housing for the intake and exhaust of air for the installation of IT equipment.

4.1.2 Current Overseas Trends

Let us examine the cooling systems adopted in the United States, which is leading the way in the construction of large-scale data centers. It was said that chiller-less water cooling systems were predominate in the United States, but outside-air cooling systems are also being adopted in an increasing number of cases. Table 2 shows trends for the data centers constructed by Microsoft, Google, and Yahoo in the past two years. It would appear that Microsoft and Yahoo have taken the lead in using outside-air cooling in most of their cooling systems. On the other hand, it has been reported that Google has constructed a data center in Finland that is fitted with a cooling system using sea water, and it seems there is no change in their policy of basing their cooling solutions on chiller-less water cooling systems.

Based on publicly available data, it is thought that the data center Yahoo opened near Niagara Falls in September 2010 follows the construction shown in Figure 2. By making use of the cool climate of Lockport where it was constructed, it seems that cooling can be achieved using outside air only for most of the year. In addition to the three companies mentioned, NetApp and HP have also adopted outside-air cooling systems in their data centers, and IIJ believes the adoption of outside-air cooling systems in data centers to be a worldwide trend. Furthermore, ASHRAE (The American Society of Heating, Refrigerating and Air-Conditioning Engineers) Technical Committee 9.9 eased data center temperature and humidity requirements in 2008 to reduce the power consumed by data centers. IIJ believes that this is one of the primary factors driving the move toward outside-air cooling systems.

4.1.3 Proceeding with Proof-of-Concept Tests

IIJ reached the conclusion that outside-air cooling systems are currently most suitable for next-generation data centers due to merits such as their energy savings, investment cost, and operational cost, as well as overseas trends. Although such systems have been implemented overseas, in order to provide them commercially in Japan's hot and humid climate it was decided that testing was required to determine whether they could withstand real-world operation here. This led to the proof-of-concept tests currently being carried out.

Table 2: Trends in the Data Centers Constructed Recently by U.S. Companies (Created by IIJ from Press Material)

Company Name	Location	Area	Date of Operation/Construction	Characteristics	Cooling System
Microsoft	Northlake Illinois, US	51,097 m²	Began operation in September 2009	PUE=1.22 1st floor uses a container system, 2nd floor uses a conventional system	Water cooling
	Quincy Washington, US	9,290 m²	Construction of an expansion began in May 2010	Flywheel UPS/IT PAC PUE=1.06	Outside air
	Dublin, Ireland	28,150 m²	Began operation in July 2009	PUE1.25	Outside air
Google	Hainaut, Belgium	Not known	Began operation in 2008	PUE=1.1	Water cooling (chiller-less)
	Hamina, Finland	8,000 m²	Begins operation in Spring 2011	Remodeled a paper mill	Sea water cooling
Yahoo	Omaha Neblasca, US	27,871 m²	Began operation in 2009	flywheel UPS	Outside air + chiller
	Lockport New York, US	14,400 m²	Began operation in September 2010	PUE 1.08 flywheel UPS	Outside air

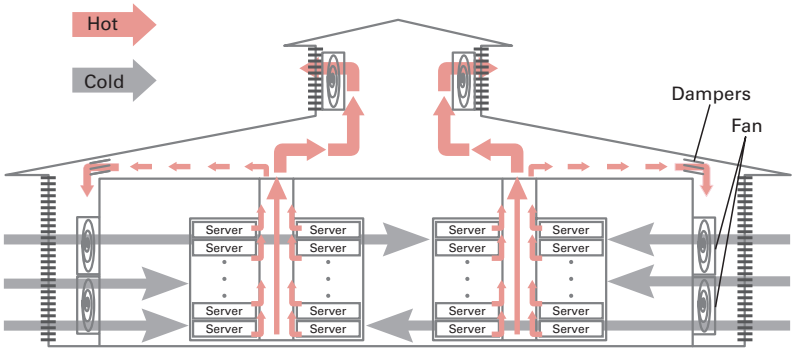


Figure 2: Yahoo Lockport Data Center Construction (IIJ Estimate)

4.2 Proof-of-Concept Test Goals and System Configuration Overview

The goal of these tests is to verify whether IT equipment such as servers can be cooled using outside air, but the ultimate objective is energy conservation, with the aim of adopting this system for commercial data centers constructed in the future. Rather than simply using outside air to cool IT equipment and determining if this was feasible or not, we needed to quantitatively measure whether such a system achieves energy conservation and can withstand use in a commercial data center.

For this reason, IIJ forged ties with professionals and partners in a number of fields when devising the system for proof-of-concept tests. Together with Toshiba Corporation, we developed a cooling module that made outside-air cooling possible, optimized IT equipment cooling, and featured automated control. We asked NLM ECAL Co., Ltd., of the Nippon Light Metal Group, to produce the IT module container units to which IT equipment would be installed. As with conventional data centers, these IT modules contain racks for installing IT equipment, and power distribution boards for delivering power safely to each rack from the main power line. Equipment for measuring electric current and pulse signals from the watt-hour meter was also required to judge whether or not energy savings were realized. We procured these from Kawamura Electric Inc.
Fires are of particular concern at data centers, which consume large amounts of power. Consequently, equipment for detecting fires in advance and extinguishing any fires that occur with minimal effect on IT equipment is required. As large amounts of air flow generally passes through data centers, the proof-of-concept test system also recreates this environment. This means that the fire detection devices used in conventional offices would not be suitable, so we installed fire warning sensors and tested whether fires within the IT module could be detected. To achieve this we collaborated with Nohmi Bosai, Ltd. Additionally, to recreate an actual data center environment as faithfully as possible, we procured and installed server equipment from KSG Company to serve as the thermal load in the IT module.

Here, we will explain the elements that make up this proof-of-concept test system. First we will provide an overview of the energy indicator for data centers.

PUE (Power Usage Effectiveness) is a metric provided by U.S. industry association The Green Grid, and is the most commonly-used indicator of data center power consumption around the world. However, for the proof-of-concept test system we are using this time, we will not be constructing the data center's equipment or systems in their entirety. For this reason, we decided to introduce the PPUE (Partial PUE) concept. As the name suggests, PPUE indicates the partial PUE for data centers, which continue to migrate towards modular systems such as those using container units. We installed watt-hour meters and other devices in our proof-of-concept test system to make it possible to calculate PPUE using the following formula.

$$\text{PPUE} = \frac{\text{cooling module power consumption} + \text{IT module power consumption}}{\text{IT module power consumption}}$$

Data Center PUE Energy Indicator

• PUE (Power Usage Effectiveness)

— The most commonly-used indicator of data center power consumption around the world, provided by the U.S. industry association The Green Grid

— Formula

$$\text{PUE} = \frac{\text{overall data center power consumption}}{\text{IT equipment power consumption}} = \frac{\text{(IT equipment power consumption + additional equipment power consumption)}}{\text{IT equipment power consumption}}$$

— When the power consumption of additional equipment is 0, the PUE is 1.0, which is the theoretical optimal level

— The average PUE of data centers in Japan is said to be about 2 (with IT equipment accounting for half of the power consumed)

— A PUE of 1.2 or less has not yet been achieved by commercial services in Japan

- Reference example -
The PUE for a data center in which servers consume 100 units of power, and other equipment (such as cooling) consumes 80 units of power

$$\text{PUE} = \frac{\text{IT 100 + Other 80}}{\text{IT 100}} = 1.8$$

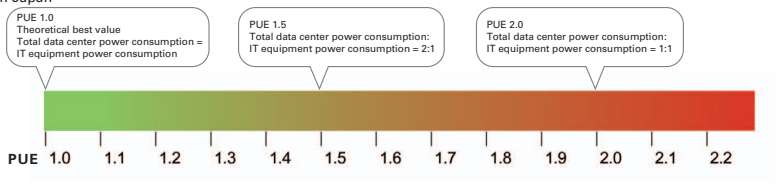


Figure 3: Data Center PUE Energy Indicator

4.2.1 The Cooling Module

As demonstrated above, the cooling module readied for our proof-of-concept tests makes outside-air cooling possible, optimizes IT equipment cooling, and features automated control. We will now examine the type of environment assumed for the optimization of IT equipment cooling. In this case we elected to adopt the temperature and humidity requirements recommended for data centers by ASHRAE (The American Society of Heating, Refrigerating and Air-Conditioning Engineers) Technical Committee 9.9 (henceforth ASHRAE 2008).

The graph in Figure 5 is a basic psychrometric chart showing dry-bulb temperature [°C] on the horizontal axis, and absolute humidity [kg/kg (DA)] on the vertical axis. The most commonly-used psychrometric chart in the cooling industry is the h-x chart, in which h = specific enthalpy [kJ/kg (DA)] and x = absolute humidity [kg/kg (DA)]. Psychrometric charts show the relationships between dry-bulb temperature [°C], wet-bulb temperature [°C], dew point temperature, absolute humidity [kg/kg (DA)], specific enthalpy [kcal/kg (DA)], and relative humidity based on atmospheric pressure (101.325kPa), and it is possible to chart all of these values as long as any two can be determined.

Next, we will explain the three operating modes operating modes of the cooling module.

■ Outside-Air Operating Mode

Outside-air operating mode is the most basic operating mode. In this mode, when the temperature and humidity of outside air are within the targeted levels set in ASHRAE 2008, outside air is used as-is to cool IT equipment, and all exhaust air from IT equipment is discarded. When operating in this mode the only power required for the cooling module is the fans for taking in outside air, making significant energy savings possible.

■ Mixed Operating Mode

Mixed operating mode is mostly used during the winter season, when the outside air has low temperature and humidity. In this mode, outside air and IT equipment exhaust air are mixed using variable blend ratios depending on the temperature and humidity of each source to create air within the targeted ASHRAE 2008 levels.

When the mix point falls below the ASHRAE 2008 range on the psychrometric chart, in other words when there is a lack of humidity, vaporizer-type humidification is implemented. As vaporizer-type humidification also removes heat from the air, the air condition transitions from the lower right to the upper left on the psychrometric chart. This makes it possible to supply air within the ASHRAE 2008 levels to IT equipment. Additionally, unlike steam humidification, vaporizer-type humidification requires no power. This means that like the outside-air operating mode the only power needed in the cooling module is for the fans, resulting in significant energy savings.

■ Circulation Operating Mode

At times it becomes impossible to create air flow within the ASHRAE 2008 levels using outside air as-is or by mixing it with IT equipment exhaust air and carrying out vaporizer-type humidification. In this case conventional cooling methods must be used, requiring the operation of cooling units such as compressors that consume large amounts of power. These functions cannot be completely overlooked simply because they have high power consumption. For this reason, in order

Partial PUE

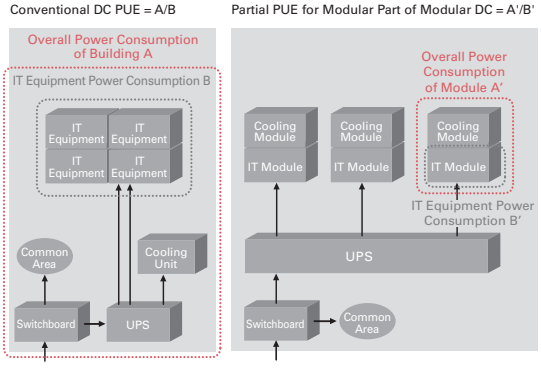


Figure 4: Partial PUE (PPUE)

	Dry-Bulb Temperature	Relative Humidity	Dew Point Temperature	Notes
ASHRAE class 1 & 2 recommended level (2008 version)	18 - 27°C	60% or less	5.5 - 15°C	The recommended equipment intake temperature and humidity levels revised by ASHRAE in 2008 to reduce data center energy consumption.
ASHRAE class 1 allowable level	15 - 32°C	20 - 80%	17°C or less	The allowable levels set to extend the period that economizers such as outside air could be used. However, the usable period depends on IT equipment testing and tolerance for hardware failure.

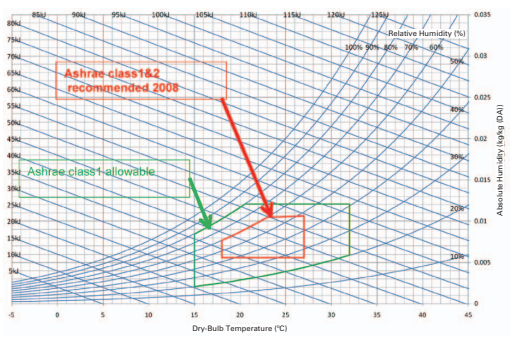


Figure 5: ASHRAE Recommended Temperature and Humidity Levels for Data Centers

to facilitate the circulation operating mode the cooling module is fitted with equipment for shutting off outside air and cooling using compressors.
The power consumed in circulation operating mode depends on the cooling ability of the compressors. For this reason, the questions of what level of product to use and whether they can be controlled to keep the use of circulation operating mode to a minimum are important points to consider to achieve total energy savings throughout the year.

The operating modes detailed here are controlled automatically via a control unit installed within the cooling module, and are transitioned between based on outside air conditions.

Next, we will discuss the components required for the cooling module.

The fans for carrying air to the IT equipment (IT module) allow inverter control, and have a maximum airflow of 27,000m3/h. Vaporizer-type humidification is achieved through the installation of humidifier modules within the cooling module wind tunnels that are supplied with water when necessary. The cooling module has multiple dampers for outside air intake, IT equipment exhaust air, and mixing outside air and IT equipment exhaust air. The blend ratio is regulated through inverter control of the aperture of these dampers. The cooling units used when in circulation operating mode consist of four outdoor compressor units each with 28kW cooling ability installed to the cooling module exterior, connected to cooling coils in the cooling module wind tunnels by refrigerant pipes. The outdoor compressor units allow for both fine control and energy savings using inverter control. Sensors for measuring temperature and humidity are installed to necessary locations both inside and outside the IT module.
A DDC (Direct Digital Controller) for controlling each of these components is installed within the cooling module, performing a variety of control functions such as automated control of each operating mode. In addition to these components, medium efficiency particulate air filters are installed in the cooling module due to the use of outside air, filtering out dust particles of 0.5μm or larger.

For the proof-of-concept tests the cooling module and outdoor compressor units have also been designed with surplus size. The cooling modules and outdoor compressor units for commercial data centers to be built in the future are expected to be about 2/3 the size of those used in the proof-of-concept tests.

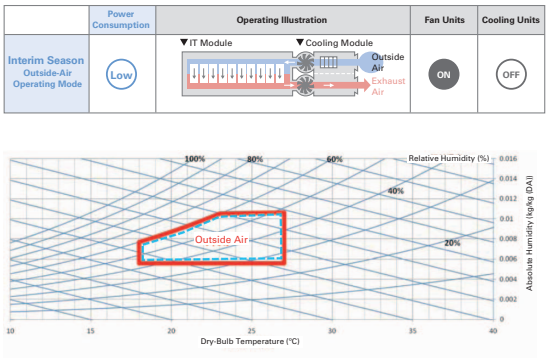


Figure 6: Outside-Air Operating Mode

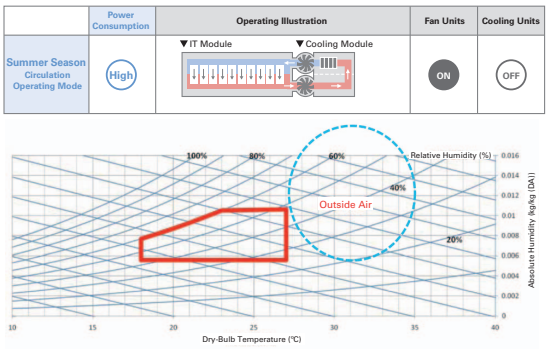


Figure 8: Circulation Operating Mode

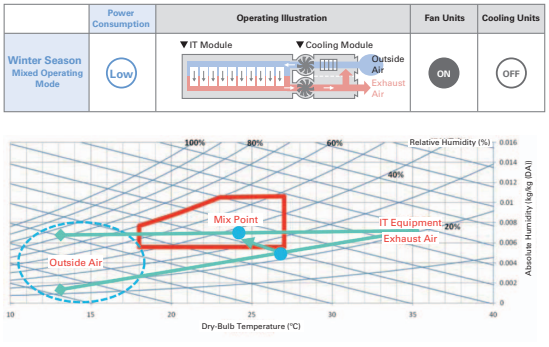


Figure 7: Mixed Operating Mode

Figure 9: From Left - Outdoor Compressor Units, Cooling Module, and IT Module

4.2.2 The IT Module

The container unit for housing IT equipment such as servers is called the IT module. The interior of the IT module is divided into cold area in front of the racks that house IT equipment and the hot area behind them. The cooling module and IT module are connected by two air ducts, with air suitable for cooling the IT equipment sent from the cooling module to the IT module cold area, and exhaust air from the IT equipment returned to the cooling module from the IT module hot area.

For the proof-of-concept tests we set a thermal load of 90kVA for IT equipment such as servers. In the age of cloud computing, data centers must have high-density capacity for housing IT equipment, so we aimed for effective power of 10kVA per rack. We considered that an IT module fitted with nine racks should make for a usable effective power of 90kVA.

However, the purpose of these proof-of-concept tests is only to verify the operation of a cooling system using outside air cooling, and IT equipment is only introduced to serve as the thermal load. For this reason, we explored various options before beginning actual construction. The racks we prepared each had approximately 40U of space for installing heat sources, with consumption of 250VA of power consumption necessary for each 1U of space. To prepare this thermal load inexpensively, one possible solution would be to use a set of light bulbs. If 10 x 100W incandescent bulbs could be installed in 4U of space, it would be possible to achieve a load similar to that necessary. It is possible that hot plates (approximately 1300W), table heaters (approximately 500W), or dryers (approximately 1200W) could also be used. However, all of these devices are difficult to control externally, and for constant 24-hour operation fire hazards become a concern. There is also concern with regard to air flow, as each pieces of IT equipment is fitted with fans. For this reason, it was judged that unless this air flow could be recreated the equipment would not be suitable for proof-of-concept tests, even if its purpose was simply to create a thermal load.

After considering these factors, in the end we decided to carry out proof-of-concept tests with actual IT equipment (servers) installed. We intentionally used second-hand server equipment of about five years old to reduce the procurement cost and generate the power consumption for each 1U of space. Newer servers have more power saving features, so slightly older servers tend to consume more power. We installed multiple server models from a variety of manufacturers. Most of the servers had a rated value of 300 to 400VA in their catalog specifications, but actual power consumption averaged out to approximately 180 to 200VA. We used mainly 1U servers, and by fitting each with two CPUs, the maximum number of memory modules (with a focus on number of modules rather than amount of memory), and two HDDs, we managed to raise the power consumption per 1U to 250VA, attaining the maximum 90kVA for the IT module overall.

Although each server merely serves to contribute to the thermal load, we made it possible to control them remotely by installing operating systems and connecting them to a network. With only the OS running and no processing load the power consumption of servers was about 70% (approximately 60 to 65kVA for the IT module overall), and with benchmark tool processes running the load could be increased to 100% (approximately 90kVA). Also, when installing the servers we raised cooling efficiency as much as possible by covering the gaps between racks with masking tape.

Many other refinements were applied to the IT module. In particular, a large amount of sensor equipment was installed to allow a variety of data to be obtained.

Figure 10: Masking Tape Applied Between Racks to Raise Cooling Efficiency

4.2.3 PPUE Simulation

As detailed above, we constructed a cooling module with three operating modes that are each controlled automatically to supply air within ASHRAE 2008 levels to IT equipment, and an IT module that produces a maximum thermal load of 90kVA. Before discussing the actual results of our proof-of-concept tests, we will present the results of a simulation we carried out to estimate the PPUE when the proof-of-concept test system was used.

The Japan Meteorological Agency releases meteorological statistics such as past temperatures and humidity levels for the various regions of Japan. By plotting this data on a psychrometric chart such as the one in Figure 11, it is possible to calculate the yearly operating hours for each operating mode of the cooling module.

Additionally, as the power consumption of each of the cooling module's operating modes is already known, we can use this data to calculate on paper the PPUE of the proof-of-concept test system if it were used in various locations in Japan. Figure 12 shows the results of this simulation. As Figure 12 demonstrates, a lower PPUE can be expected for colder areas in the north. However, with the exception of Okinawa (Naha), the fluctuation in PPUE was within 0.1 throughout Japan. Meanwhile, when facilities are constructed in colder areas, frosting prevention and snow damage countermeasures are required for the winter season, possibly leading to an increase in initial investment and running costs. Accordingly, it is not as simple as installing the outside-air system used for these proof-of-concept tests in a cold location throughout the year.

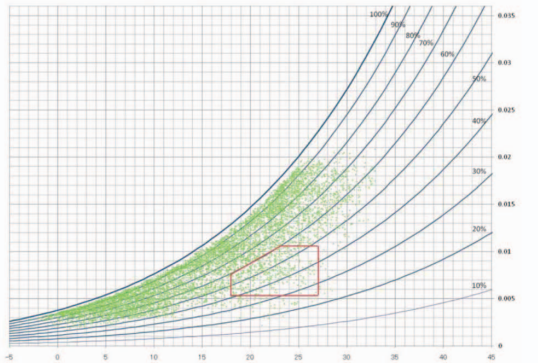


Figure 11: An Example of Outside-Air Temperature and Humidity for Matsue (2009) Plotted on a Psychrometric Chart

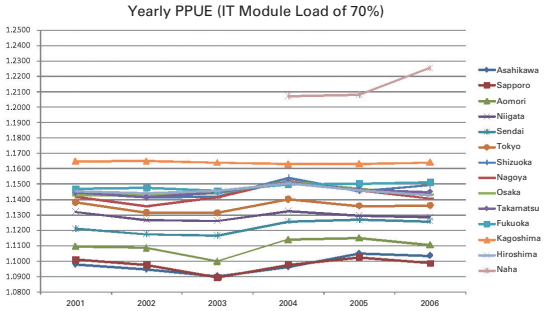


Figure 12: Simulation Results

4.3 Proof-of-Concept Test Results and Discussion

We have already gathered a variety of data from the proof-of-concept tests begun in February 2010 and applied this feedback to the commercial modules. Here, we detail and discuss the results of the proof-of-concept tests based on operating data for the cooling module.

4.3.1 Cooling Module Power Consumption

Power consumption for the cooling module can be divided into that for the SA (supply air) fan and that for the outdoor compressor units. Technically, the power consumption for control equipment should also be added to this, but as the amount is insignificant it is not mentioned here.

■ SA Fan Control

The SA fans supply cold air from outside or generated by the outdoor compressor units to the cold area in the IT module, and return the IT equipment exhaust air expelled into the hot area to the cooling module. As they operate throughout the year, SA fan efficiency has a significant effect on cooling module energy savings.

By lowering the rotation speed of the SA fans and reducing the air flow, their power is reduced proportionally to the third root of the rotation speed. In other words, if air flow is reduced to 1/2, power is reduced to 1/8. Because the air flow supplied to cold area by SA fans is controlled by adjusting the fan motor rotation speed through inverter control, it is possible to produce significant energy savings by supplying the cold area with the minimum amount of air flow necessary to cool IT equipment.

Furthermore, because IT equipment takes in air from the cold area with its own fans and exhausts this into the hot area, the SA fans require constant air flow equal to the total air flow of IT equipment fans. If the air flow of the SA fans is less than the total air flow of the IT equipment fans, a short circuit will be caused on the IT equipment. If the air flow is higher than the total air flow of IT equipment fans, the wasted air may pass through the IT equipment or gaps between the racks. Consequently, as shown in Figure 13, the most energy efficient operation is achieved when the air

flow of SA fans and the total air flow of IT equipment fans are equal. However, it is not easy to calculate the total air flow of IT equipment fans because IT equipment can be fitted with a variety of fans depending on the model, and air flow may vary based on the operating state of the IT equipment (CPU or HDD usage) and the air intake temperature (cold area temperature), such as when the rotation speed of the fan is raised to prevent overheating. For this reason, it was necessary to implement a control system in the cooling module for automatically determining variations in IT equipment fan air flow and adjusting SA fan air flow accordingly.

■ Outdoor Compressor Unit Control

Outdoor compressor units are put into operation for the circulation operating mode that does not use outside air. Outdoor compressor units are generally used to cool hot air returned from the IT module, but when the situation calls for it they can also be used to cool and dehumidify hot and humid outside air. The motors for the outdoor compressor units are controlled using an inverter, allowing fine adjustments and linear control over the temperature and humidity of the cold area by modifying cooling ability to match the IT module load. As IT equipment only produces sensible heat (changes in temperature), the cooling module is designed to have a high sensible heat ratio such as those in building-type data centers.

4.3.2 Proof-of-Concept Tests for Outside-Air Operating Mode and Mixed Operating Mode

Between February and May a wide range of data was obtained for the mixed operating mode and outside-air operating mode. Here we will present results based on proof-of-concept tests carried out on April 6. Figure 14 shows the operating report for April 6.

Because the outdoor compressor units are not operational during outside-air operating mode and mixed operating mode, the majority of power for the cooling module is consumed by the SA fans. As explained earlier, by controlling the SA fan air flow (average air flow of 14,627m3/h on April 6) efficiently with inverter control, the minimum necessary operation is carried out. Because of this, as shown in Figure 15 the power consumption of the cooling module is 4% of total power, resulting in a PPUE of 1.044. We recorded PPUE of 1.04 to 1.07 in outside-air operating mode and mixed operating mode on other days, achieving the amount of energy conservation that we expected.

Figure 16 shows temperature and humidity data for the cold area (blue), hot area (red), and outside air (green) plotted on a psychrometric chart in five second increments. The cold area (blue) plotted to 97.84%, which is within

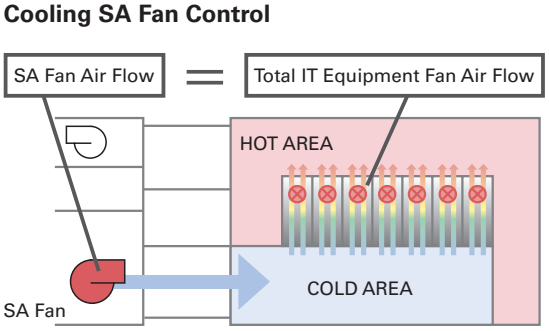


Figure 13: Most Efficient and Energy Saving Air Flow Relationship

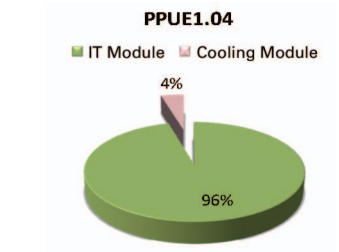
■Power Consumption
IT Power Consumption : 1550.0 kWh (Average 64.6 kW)
Cooling Power Consumption : 68.0 kWh
PUE : 1.044

■Cooling Operating Mode
1. Outside Air : 29.4% 7 hrs 2 mins
2. Mixed : 70.6% 16 hrs 56 mins
3. Circulation : 0.0% 0 hr 0 min

■Fan Air Flow (SA)
Air Flow Max: 18553 m3/h / Min: 12727 m3/h / Average: 14627 m3/h
Water Supplied to Humidifier: 0.00 m3

■Outside Air Condition
Max Temperature: 23.5°C / Min Temperature : 12.3°C / Average Temperature : 17.0°C
Max Humidity : 92.7% / Min Humidity : 43.5% / Average Humidity : 71.8%

Figure 14: April 6 Operating Report



IT Module Power	1550.0kW-h	Average 64.6kW (Average 7kVA/rack)
Cooling Module Power	68.0kW-h	Average 2.8kW
PUE (PPUE)	1.044 ((1550kW-h + 68kW-h) ÷ 1550kW-h)	

Figure 15: April 6 PPUE

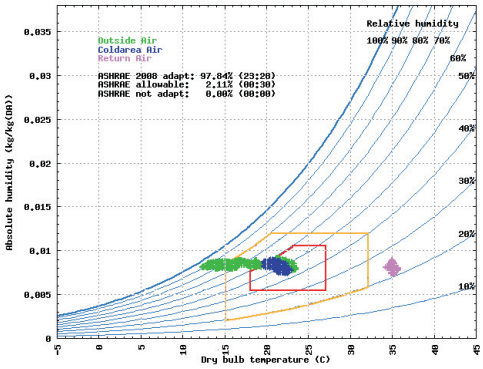


Figure 16: April 6 Psychrometric Chart

ASHRAE 2008 recommendations, and the others were also within the ASHRAE allowable levels. In other words, the temperature and humidity of the cold area remained stable throughout the day.

Furthermore, as shown in Figure 17, temperature and humidity were stable even when transitioning between mixed operation mode and outside-air operation mode, falling within ASHRAE 2008 recommended levels.

In outside-air operating mode and mixed operating mode, temperature and humidity are adjusted via damper control as shown in Figure 18. Data from the temperature and humidity sensors installed in the cold area are obtained by the DDC (Direct Digital Controller) in real time, and the apertures of the outside air intake damper, exhaust heat damper, and mixed damper are adjusted. The fact that temperature and humidity remain stable within ASHRAE 2008 levels during the proof-of-concept tests indicates that damper control is being executed appropriately.

Humidification control is also an essential function in outside-air operating mode and mixed operating mode. Figure 19 shows the operating report for April 30. On this day the absolute humidity (the amount of water vapor included in 1kg of dry air) of the outside air was low, so the vaporizer-type humidifier was activated to bring the cold area temperature and humidity within ASHRAE 2008 levels.

A vaporizer-type humidifier flushes water over the top of humidifying materials, humidifying air that passes over through natural evaporation. Figure 20 shows the psychrometric chart for April 30. The cold area (blue) plotting remains within ASHRAE 2008 levels, demonstrating that humidification control is being carried out appropriately without causing an excess or lack of humidity.

4.3.3 Circulation Operating Mode

Between June and August we gather a variety of data regarding the circulation operating mode. Here we will report on results based on proof-of-concept tests carried out on July 6. Figure 21 shows the operating report for July 6. Circulation operating mode was used throughout the entirety of the day.

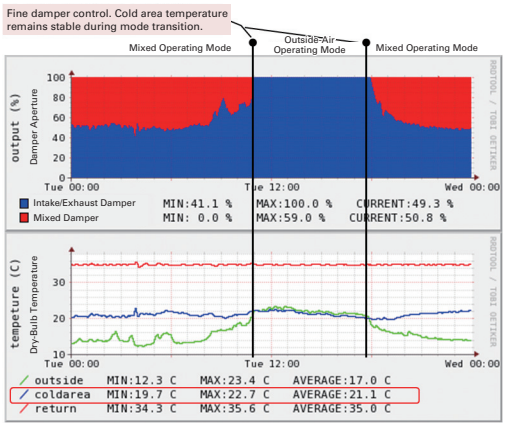


Figure 17: Damper Aperture and Temperature Transition

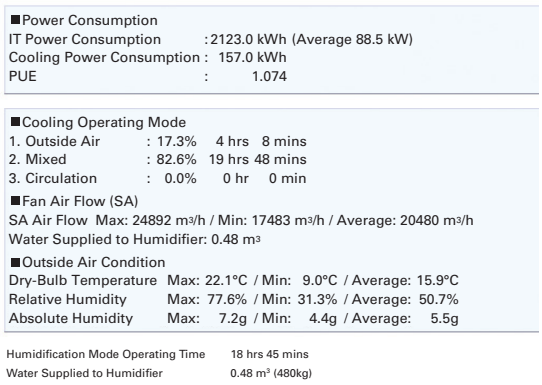


Figure 19: April 30 Operating Report

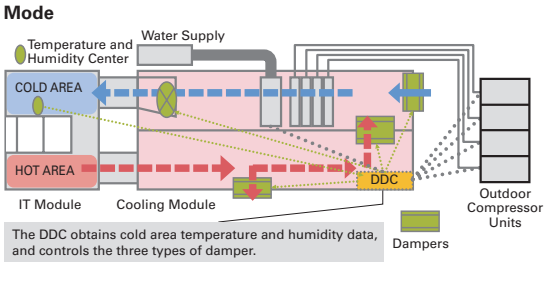


Figure 18: DDC and Dampers

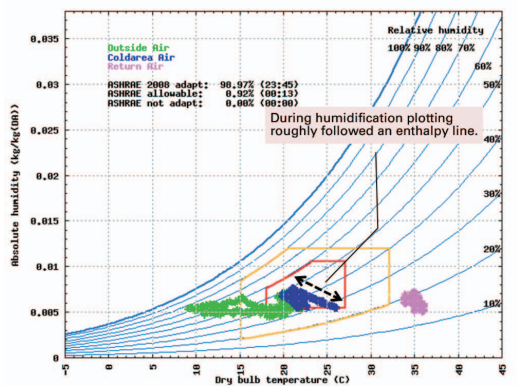


Figure 20: April 30 Psychrometric Chart

As shown in Figure 22, cooling module power on July 6, which had a maximum outside air temperature of 30.6°C, an average temperature of 27°C, and an IT module load of 63.7kW (70% of the maximum 90kW), was 22% of total power, resulting in a PPUE of 1.284. On days other than July 6 that circulation operating mode was used, PPUE between 1.24 and 1.30 were recorded. The reason for the large fluctuation in PPUE is the fact that the power required by the outdoor compressor units varies depending on outside air temperature and humidity as well as IT module load.

Figure 23 shows the psychrometric chart for July 6. The cold area temperature and humidity (blue) stayed within ASHRAE 2008 levels. Also, as shown in Figure 24, the temperature, relative humidity, and absolute humidity of the IT module cold area and hot area remained stable.

In circulation operating mode, efficient operation is made possible by shutting off outside air. Additionally, in the event that outside air with high humidity and temperature is admitted, the outdoor compressor units are fitted with functions for dehumidifying and cooling air to prevent violent fluctuations in the IT module's temperature and humidity levels. We also experimented with different output levels and numbers of operating outdoor compressor units, as well as multiple operation patterns, and implemented functions allowing the DDC to control the outdoor compressor units to consume the least total power (Figure 25).

■Power Consumption

IT Power Consumption	:	1529.0 kWh (Average 63.7 kW)
Cooling Power Consumption	:	434.0 kWh
PUE	:	1.284

■Cooling Operating Mode

1. Outside Air	: 0.0%	0 hr	0 min
2. Mixed	: 0.0%	0 hr	0 min
3. Circulation	: 99.9%	23 hrs	59 mins

■Outside Air Condition

Dry-Bulb Temperature	Max: 30.6°C	Min: 25.5°C	Average: 27.0°C
Relative Humidity	Max: 99.5%	Min: 68.2%	Average: 89.9%
Absolute Humidity	Max: 22.2g	Min: 18.1g	Average: 20.3g

Figure 21: July 6 Operating Report

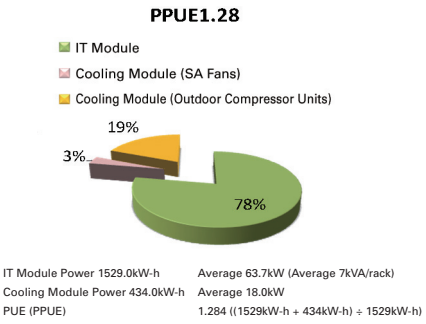


Figure 22: July 6 PPUE

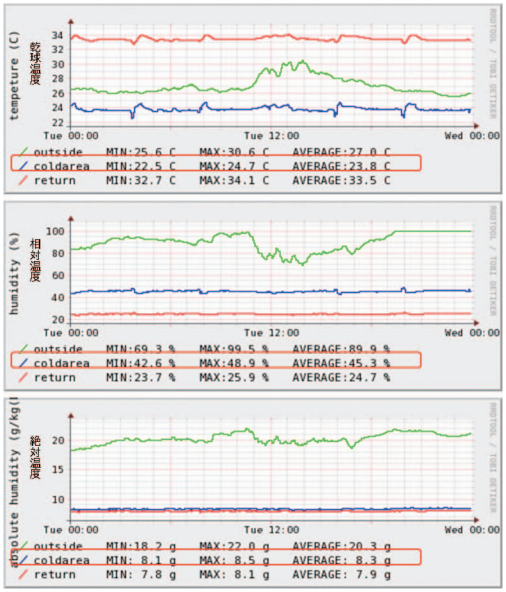


Figure 24: Dry-Bulb Temperature, Relative Humidity, and Absolute Humidity Changes

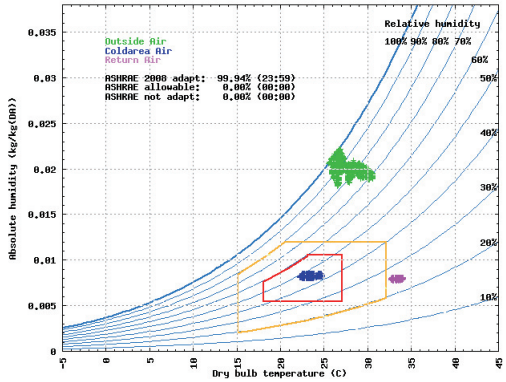


Figure 23: July 6 Psychrometric Chart

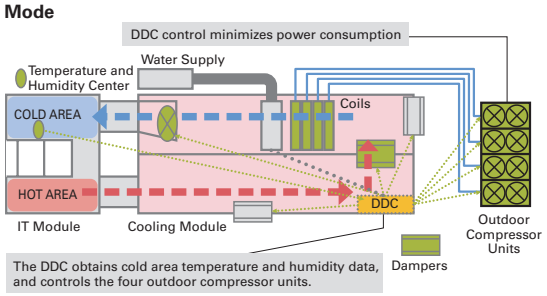


Figure 25: DDC and Outdoor Compressor Units

4.4 Future Considerations

4.4.1 Working Toward Further Energy Savings

Although we now have a clearer idea of the energy savings that an outdoor-air cooling system can provide, we plan to consider and evaluate steps such as the following in the medium- and long-term, with the aim of making further energy savings.

STEP 1 Expansion of existing systems (for example, reducing power consumption by using outside-air operating mode in the summer season as well).
STEP 2 Integration of cooling equipment and IT equipment (for example, due to both cooling equipment and IT equipment having their own fans with separate temperature control, integrating control would reduce the double-up of fans).
STEP 3 Realization of a carbon neutral data center (for example, creating a system enabling energy use without generating CO_2 through the integrated construction and operation of power plants that utilize natural energy (wind power, solar power, etc.) and data centers.

First of all, as part of step one we will provide an overview of the proof-of-concept tests for summer season use of outside-air operating mode carried out in August 2010.
With the cooperation of a number of IT equipment vendors, we carried out tests using outside-air operating mode instead of circulation operating mode in the summer season, aiming to maintain a PPUE of 1.1 or less throughout the year. As use of outside-air operating mode was forced for a 24-hour period, the cold area became the same temperature as the outside air, resulting in a room temperature of over 35°C at its highest (which in turn led to a hot area temperature of 45°C). However, as shown in Table 3, PPUE improved significantly, going from 1.25 to 1.06. That said, total power consumption fell only 6%, going from 70kW to 66kW. This is because although cooling power consumption fell 10kW, the high room temperature caused an increase in the fan rotation speed of IT equipment, consuming an extra 6kW (server fan power consumption generally increases significantly when the intake area temperature exceeds 25°C), and resulting in overall energy savings of just 4kW. We anticipated achieving a PPUE of 1.07 by reducing the power consumption of cooling equipment while maintaining that of the IT equipment, but feel we have made significant progress by quantitatively measuring that although the PPUE may meet our expectations, it is not possible to reduce overall power consumption greatly.

We will continue to analyze the data from these tests together with IT and cooling equipment vendors, and we hope to obtain data that will contribute toward the second step of integrating IT and cooling equipment.
As has been mentioned before, PUE improvements may not necessarily lead to energy savings, and we have reestablished the fact that indicators other than PUE are necessary when pursuing the detailed refinement of energy savings.

4.4.2 Construction of the Matsue Data Center Park for Commercialization

In order to apply the technology we have proven in these tests to real-world operation, on September 1, 2010 we began work on construction of the Matsue Data Center Park as the first commercialized data center using outside-air cooled container units in Japan, with the aim of beginning operations in April 2011. We received backup in the form of investment aid and electric utility fee assistance based on the government's industrial development policies.
This data center park integrates building, electrical equipment, cooling equipment, and IT equipment resources in modular form to meet the needs of cloud services. The first-generation Matsue Data Center Park will be the facility the IIJ GIO cloud service is based on, and as Japan's first container-based data center it will offer low cost solutions, high server capacity, and easy scale-out with the following principle features.

- Utilizes an outdoor-air cooling system
- Utilizes the IZmo (patent pending) IT modules we have developed in-house
- Features efficient placement of data center components

The Matsue Data Center Park implements a highly efficient outdoor-air cooling system based on the results of our proof-of-concept tests. Facility costs for the IT modules have been lowered by integrating the ducts that supply

Table 3: Summer Season Circulation Operating Mode and Outside Air Operating Mode

	Circulation Operating Mode	Outside-Air Operating Mode		
	Actual Value	Expected Value	Actual Value	
IT Equipment Power Consumption	62kw	56kw +6kw	62kw	Fan rotation speed rises, increasing power consumption
Cooling Equipment Power Consumption	14kw −10kw	4kw	4kw	Power consumption is above expected values
Total	70kw −4kw	60kw +6kw	66kw	
Partial PUE	1.25 −0.19	1.07 −0.01	1.06	PUE was lower than expected values

outside air and module housing. Cooling efficiency has also being raised by separating the hot area and cold area inside the modules, and all racks support effective power consumption of up to 10kVA, reducing running costs such as electric utility fees. On top of this, we are installing racks at an angle within the modules to keep the IT module width within 2.5m while securing the necessary amount of interior space. These measures make it possible to transport the modules using standard heavy trucks rather than requiring a special vehicle such as a trailer, reducing transport costs by roughly 1/3.

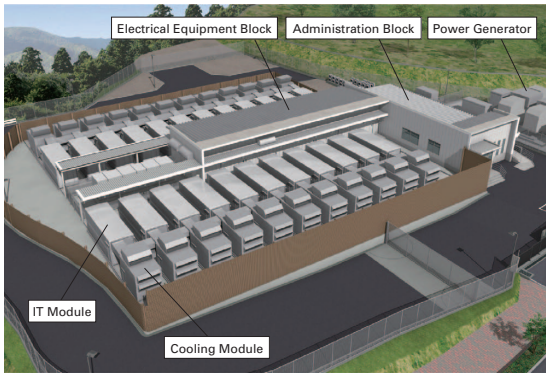


Figure 26: Matsue Data Center Park Illustration

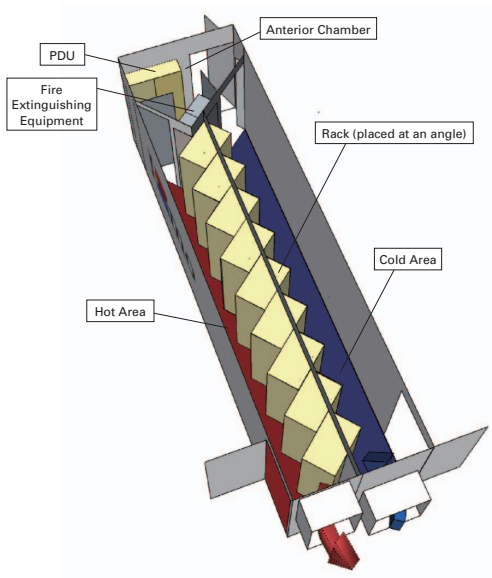


Figure 27: IZmo IT Module Illustration

The Ministry of Land, Infrastructure and Transport is examining whether the containers used for the data center fall outside the scope of "buildings" as defined under Article 2 of the Building Standards Act. Being quick to take to the concept that these are equipment items rather than buildings, we have also implemented a variety of functions for remote operations such as powering on/off IT equipment and checking status lamps.

At the Matsue Data Center Park we are adopting our own original MISP (Module Inter-connection over the Shortest Path) system for the placement of electrical equipment and cooling modules in front and at back of IT modules respectively. This minimizes the connection distance of components such as power cables and refrigerant pipes, and reduces the energy loss from cable distribution while also lowering equipment investment cost.

4.5 Conclusion

The proof-of-concept tests we have carried out to achieve energy savings for data centers will first come to fruition in the construction of our first-generation Matsue Data Center Park, but we will continue our forward-thinking initiatives toward achieving the integration of cooling and IT equipment and carbon neutral data centers while building up our commercial operations experience, and working toward the realization of our second- and third-generation data center parks.

Author:
4.1/4.4
Isao Kubo
Vice Manager, Data Center Business Planning and Operations Department, IIJ Service Division
After working at a major telecommunications carrier, Mr. Kubo joined Crosswave Communications, Inc., and implemented the interconnection of NTT dark fiber in several dozen locations across the country (a Japan first). He joined IIJ in 2008, and now oversees the operation and expansion of its existing data centers in addition to the construction of next-generation data centers.

4.2
Hideaki Kawashima
Section Manager, Planning Section, Data Center Business Planning and Operations Department, IIJ Service Division
Mr. Kawashima joined IIJ in 2002. Following work promoting the sales of SEIL/SMF and constructing large-scale solutions in the Network Integration Department, he became engaged in planning for its data center operations from 2009.

4.3
Akio Hashimoto
Planning Section, Data Center Business Planning and Operations Department, IIJ Service Division
Mr. Hashimoto joined IIJ in 2009 after working in the design, construction, and operation of communication base stations and as a facility engineer at data centers for telecommunications carriers. He is currently involved in the evaluation, design, and construction of next-generation data centers.

Ongoing Innovation

Vol.9 November 2010

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/

IIJ-MKTG020GA-1012CP-00001PR