1 Infrastructure Security

1.1 Introduction

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

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

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

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

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

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

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

1.2 Incident Summary

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

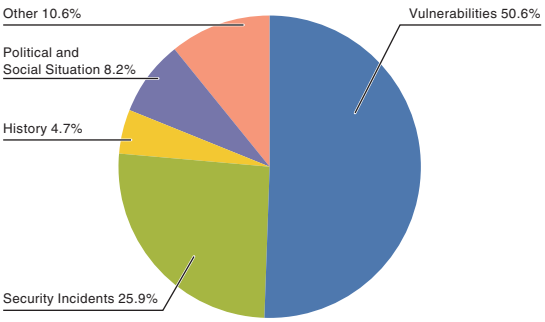


Figure 1: Incident Ratio by Category (April 1 to June 30, 2009)

Table 1: Incident Categories

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

■Vulnerabilities

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

■Political and Social Situation

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

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

■History

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

■Security Incidents

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

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

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

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

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

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

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

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

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

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

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

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

■Other

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

1.3 Incident Survey

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

1.3.1 DDoS Attacks

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

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

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

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

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

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

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

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

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

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

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

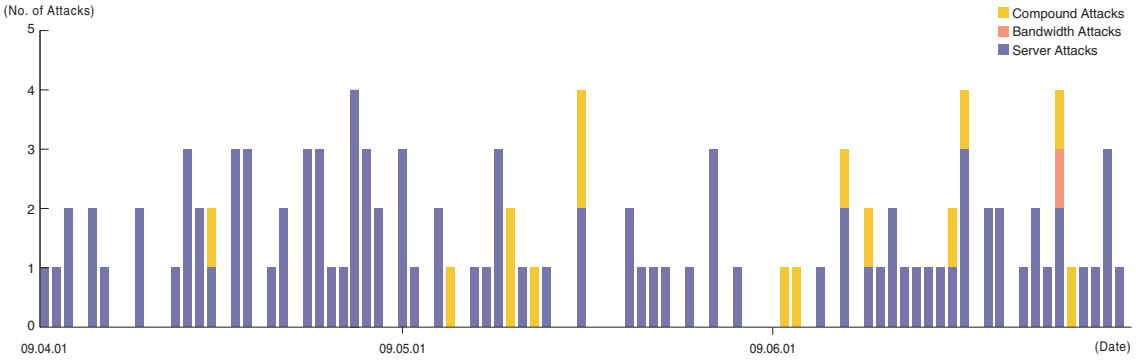


Figure 2: DDoS Attacks

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

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

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

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

1.3.2 Malware Activities

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

■Status of Random Communications

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

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

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

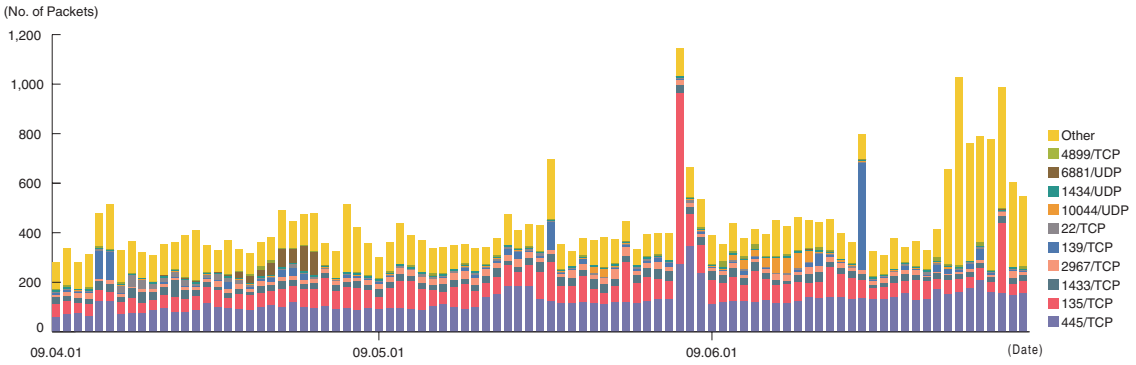


Figure 3: Communications Arriving at Honeypots (By Date, By Target Port, Per Honeypot)

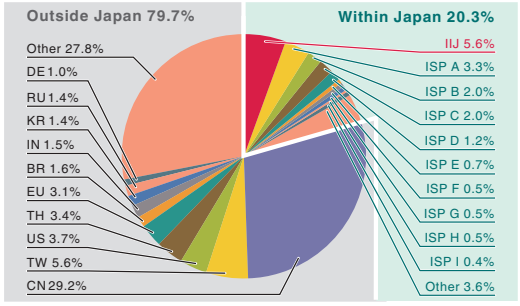


Figure 4: Sender Distribution (Entire Period under Study)

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

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

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

*22 Microsoft Security Bulletin MS08-067 – Critical, Vulnerability in Server Service Could Allow Remote Code Execution (http://www.microsoft.com/technet/security/Bulletin/MS08-067.mspx).

■Malware Network Activity

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

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

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

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

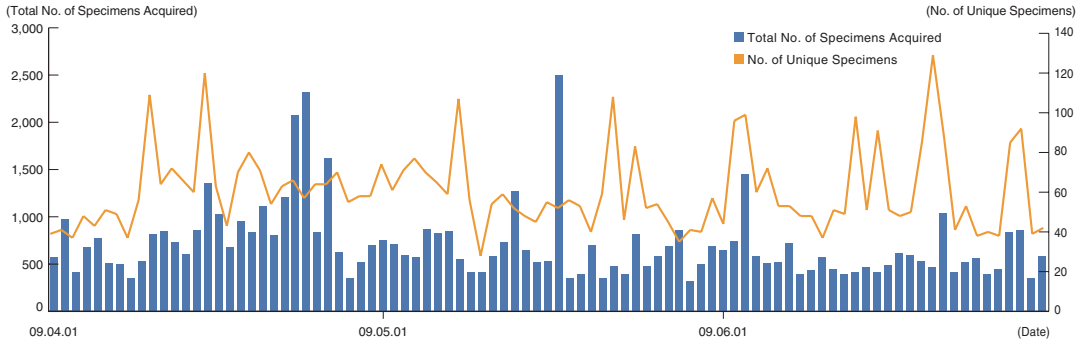


Figure 5: Trends in Number of Malware Specimens Acquired (Total Number, Number of Unique Specimens)

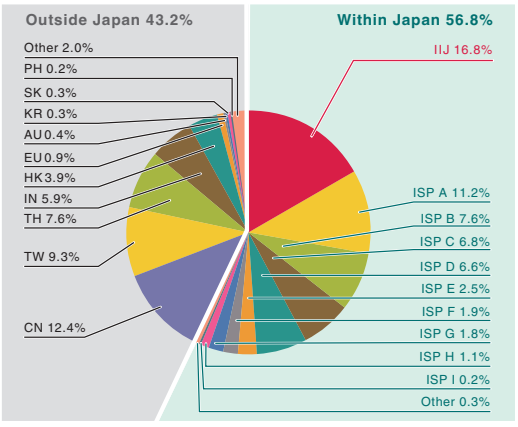


Figure 6: Distribution of Acquired Specimens by Source (Entire Period under Study)

*23 This indicates the malware acquired by honeypots.

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

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

1.3.3 SQL Injection Attacks

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

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

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

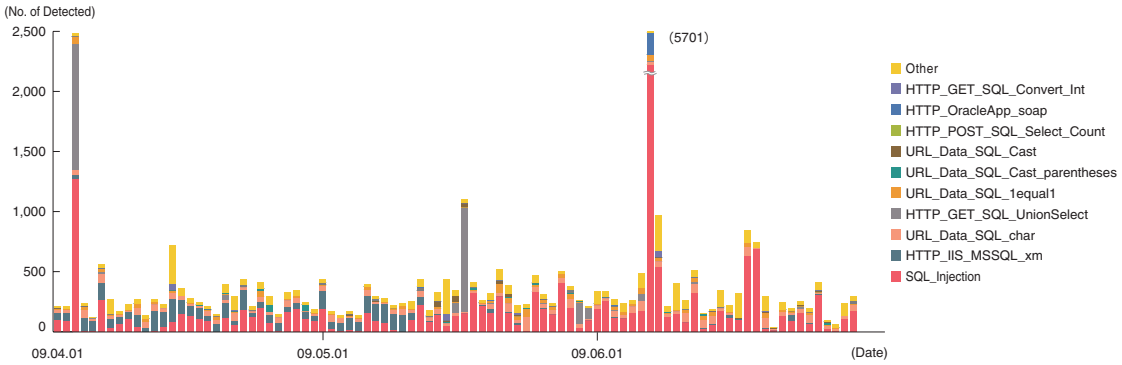


Figure 7: Trends of SQL Injection Attacks (By Day, By Attack Type)

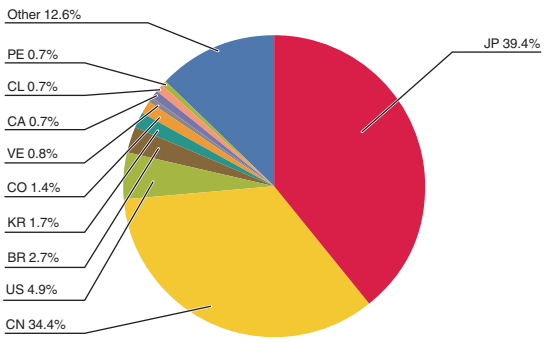


Figure 8: Distribution of SQL Injection Attacks by Source

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

1.4 Focused Research

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

1.4.1 Worldwide Outbreak of the Conficker Malware

■About Conficker

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

■Conficker Variants and Their Behavior

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

■ Infection Activity

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

■ Control and Updates

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

Table 2: Conficker Variants

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

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

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

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

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

■ Introduction of Other Malware

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

■State of Infection

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

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

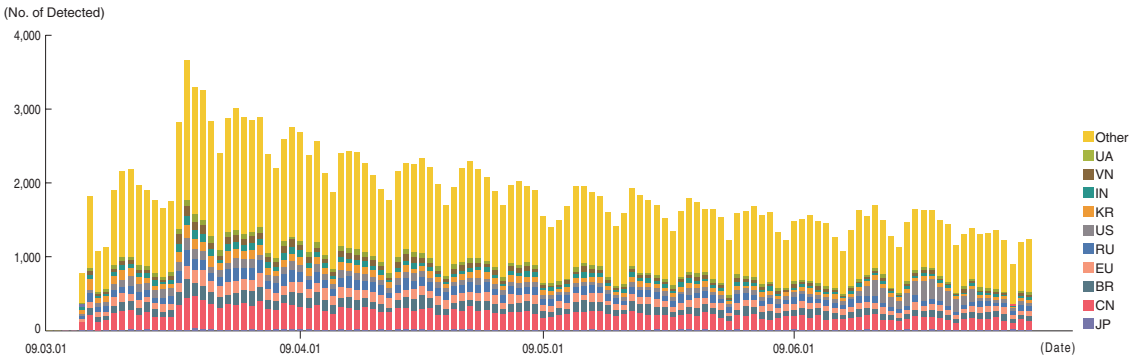


Figure 9: Conficker.D P2P Port Access (By Country)

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

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

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

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

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

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

1.4.2 ID/Password Stealing Gumblar Malware

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

■Timeline of Events

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

■ From Content Alteration to Malware Infection

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

■ Malware Behavior

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

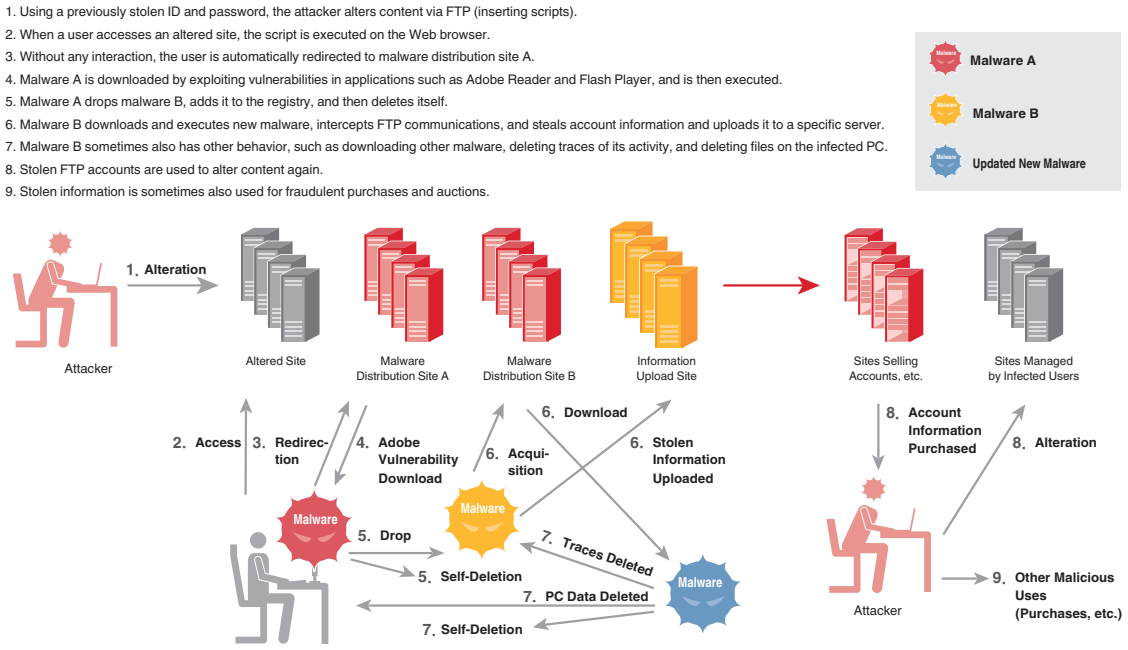


Figure 10: Anatomy of a Gumblar Incident

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

■ From Upload of Information to Exploitation

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

■Characteristics of Gumblar

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

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

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

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

■Recommendations for Users

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

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

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

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

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

1.4.3 Cloud Computing and Security

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

■About Cloud Computing

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

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

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

■Security Issues for Cloud Computing

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

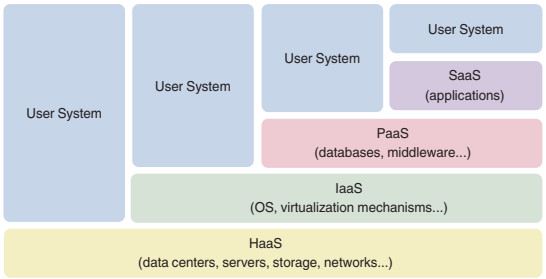


Figure 11: Layers of XaaS

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

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

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

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

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

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

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

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

■ Issues Related to Boundaries

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

■ API-Related Issues

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

■ Digital Forensics

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

■Using the Cloud Safely

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

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

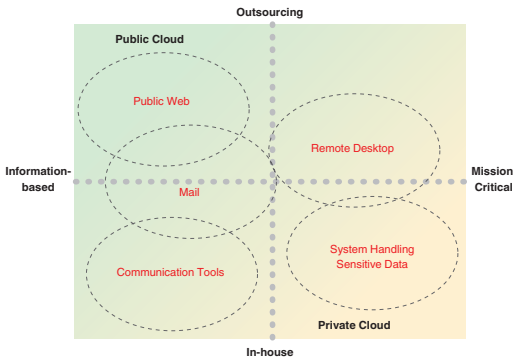


Figure 12: Proper Use of Services Based On System Purpose

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

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

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

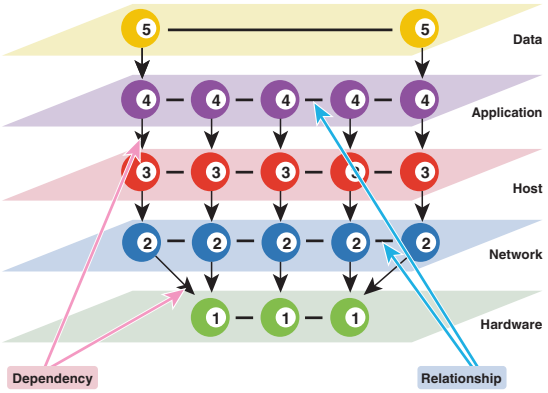
In this section, we have summarized a variety of security-related concerns with cloud computing. With the ever-advancing aggregation and optimization of information systems, opportunities to use cloud computing technology will inevitably be more frequent in the future. As indicated in this section, if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

1.5 Conclusion

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

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

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



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

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

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

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

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

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