Internet Infrastructure Review

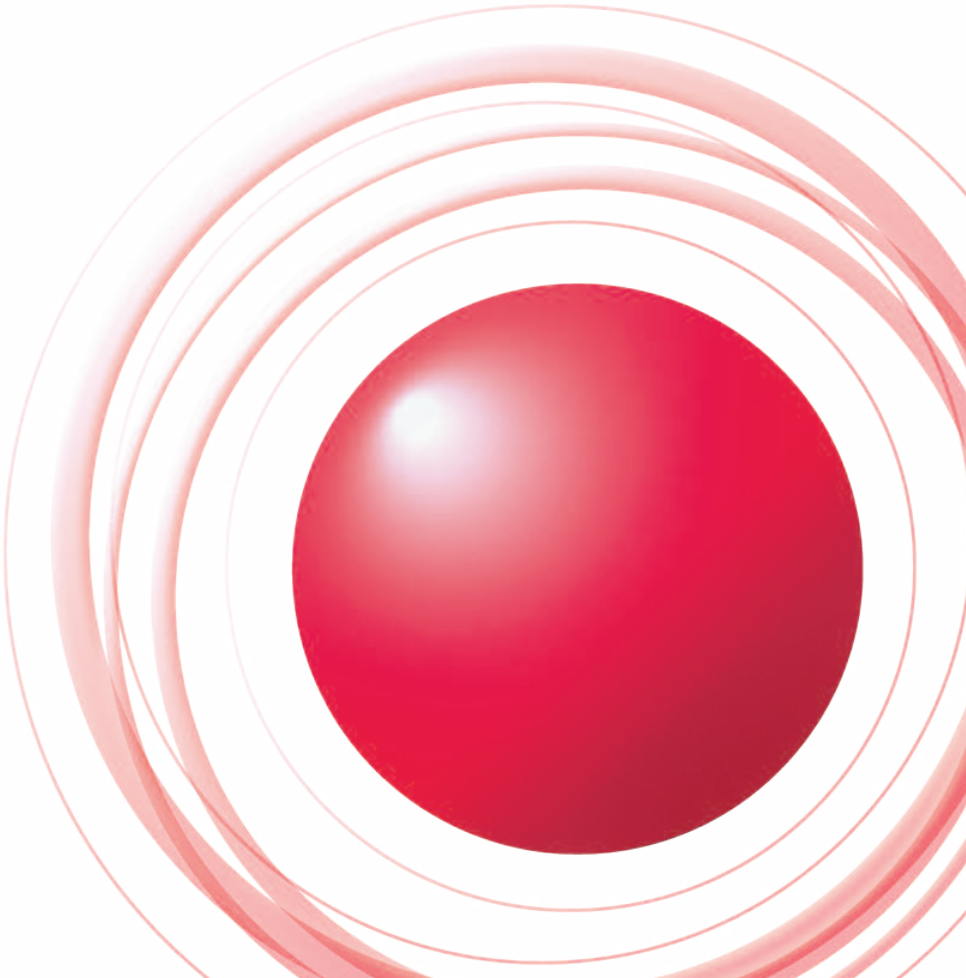
IIJ
Internet Initiative Japan

Vol.3

May
2009

Infrastructure Security
Increasingly Sophisticated Fraud

Email Technical Report
Sender Authentication Technologies DKIM



Internet Infrastructure Review Vol.3 May 2009

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

Executive Summary

While the government's economic remedies are now finally underway, the International Monetary Fund (IMF) is projecting a 6.2% decrease in real growth for the Japanese economy during fiscal 2009. Clearly, the recession will continue for the foreseeable future. According to a survey conducted by the Japan Users Association of Information Systems, 55% of companies asked forecasted lower IT investment for 2009 as compared to 2008. The survey indicated an average decrease of 10%; 2009 is shaping up to be a very difficult year for the IT industry.

According to an IDC study, the scope of the so-called cloud computing market (SaaS/PaaS/IaaS) grew at a 19.2% clip during fiscal 2008 compared to the prior year. Some estimations have this level of growth continuing through 2009 and beyond. All indications are that the global economic crisis has convinced companies to opt for IT services that are provided over the Internet on an as-needed basis. This contrasts with historic practices of developing proprietary systems, investing in capital equipment, and managing systems in-house. The shift to a pay-per-use format is an obvious effort to control overall costs, while optimizing the corporate IT environment.

This type of IT services model has been championed more than once in the past; however, we can identify several reasons as to why the practical implementation of this model is a real possibility today. First, we can point to the advancement in broadband Internet and stable network services, available at more reasonable prices than ever. Second, we have seen great strides in computer system virtualization and Web services technologies. Third, the current economic recession is serving as an added impetus for the shift toward a per-use service model.

As these trends continue apace, ensuring safety on the Internet becomes an even more important issue in terms of corporate business continuity. In this sense as well, it is vital to identify and understand the incidents and vulnerabilities that exist under the surface of the Internet cloud. Corporate IT managers need this information to be able to fairly evaluate cloud services provider service levels, and to create policies ensuring the safe use of such services.

This whitepaper summarizes technical information related to potential incidents and vulnerabilities that threaten the stable operations of the Internet as a whole, possibly preventing our client firms from using the Internet in safety and confidence.

This whitepaper consists of information from a survey report conducted over the13 weeks between January 1 and March 31, 2009. Here, we offer commentary on the survey results, looking at historical statistical data focused on SQL injection attacks (a threat to Web services), alerts related to ID and password management (indispensable for using services over the Internet), and "scareware," a recent and growing cause of damages.

During the period in question, the ratio of spam observed averaged 81.5% of all emails—remaining an extremely high percentage. We will explain in this whitepaper that thorough deployment of appropriate control mechanisms on the part of the sender is an effective action for reducing spam. We will present data to support our conclusions.

IIJ will continue to respond to all manner of incidents and vulnerabilities, actively disseminating information in order to support the further development of the Internet into a safe and stable part of the social infrastructure, particularly as the Internet becomes an even more critical component of the infrastructure underlying corporate activities.

Author
Toshiya Asaba
Executive vice president. Member of the WIDE Project. Mr. Asaba joined IIJ in its inaugural year of 1992, becoming involved in backbone construction, route control, and interconnectivity with domestic and foreign ISPs. Asaba 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 he serves concurrently as president and CEO of that organization.

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 related to services, and information obtained from companies and organizations that IIJ has cooperative relationships.

This volume (Vol.3) covers the period of time from January 1 through March 31, 2009. A number of incidents occurred during this period; we will be addressing the most representative of those in this whitepaper.

Infections of Conficker and its variants were repeatedly reported during the period in question (Conficker first came to prominence last year). A number of other incidents involved the alteration of Web content, facilitated through password theft.

Vulnerabilities that affected a wide range of systems or users have been identified, including OpenSSL vulnerabilities, problems with transparent proxy servers, etc.

The total number of malware specimens on the Internet is in decline, according to IIJ observations. While the number of DDoS attacks has likewise decreased, attacks still happen on a scale that directly affect server performance. 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 January 1 and March 31, 2009. Figure 1 shows the distribution of incidents handled during this period, while Table 1 provides an explanation of categorizations.

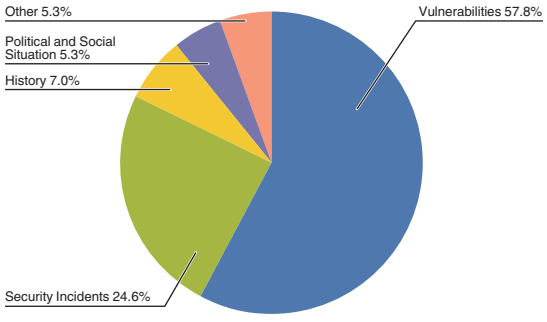


Figure 1: Incident Ratio by Category (January 1 to March 31, 2009)

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

We noted numerous vulnerabilities related to client operating systems and applications. These included the discoveries or identifications of a significant number of attack methods not relying on specific implementations or versions, including CA spoofing using MD5 vulnerabilities*1, OpenSSL vulnerabilities*2, Intel TXT security structure vulnerabilities*3, host header interpretation problems in transparent proxy servers*4, and Cisco IOS attack methods*5 using Return Oriented Programming*6.

■Political and Social Situation

The 2009 World Baseball Classic and several other international events were held during the period under study. However, IIJ did not note any attacks on IIJ facilities or client networks associated with any of these events. IIJ paid careful attention to political situation during Northern Territories Day (February 7) and Takeshima Day (February 22) [two dates observing controversial events/disputes –Ed.]. IIJ also paid careful attention during the event of the North Korean missile launch in late March. No attacks directly related to these events against IIJ facilities or client networks were detected.

■History

The period in question included several historically significant days on which multiple sites in Japan had been subject to DDoS attacks; however, IIJ did not detect any direct attacks on IIJ facilities or client networks.

■Security Incidents

The largest of unanticipated incidents not linked to political and social situation was the spread of Conficker variants*7 exploiting Microsoft Security Bulletin MS08-067. These variants infect other computers not only via the network using the MS08-067 vulnerability, but also via USB memory devices and other media, resulting in reports of compromised PCs not connected directly to the Internet. Many arguments*8 since have been put forth for disabling the Windows AutoRun feature.

We also noted an increase in alteration of Web content*9 through the theft of user account information (ID/password). See “1.4.2 Alerts Concerning ID/Password Management.”

*1 Intermediate CA certificates can be counterfeited in attacks using this method. However, such attack requires that approximately 8,000 PCs perform one or two days’ worth of calculations (http://www.win.tue.nl/hashclash/rogue-ca/).

*2 OpenSSL has issues with the validation of certain certificates; counterfeit certificates could be viewed as authentic (http://www.openssl.org/news/secadv_20090107.txt).

*3 Announcement related to the discovery of a defect allowing the bypass of Intel TXT security protections and related implementation errors (http://theinvisiblethings.blogspot.com/2009/02/attacking-intel-txt-paper-and-slides.html).

*4 When a transparent proxy exists between the Web browser and Web server, security features such as Same Origin Policy in Java implementation, may be bypassed through the host header manipulation (http://www.kb.cert.org/vuls/id/435052).

*5 Under this method, the Cisco ROMMON code is utilized to create attack code using Return Oriented Programming, allowing for the creation of version independent exploit code. This method can be a serious threat when a remotely exploitable vulnerability is discovered (http://www.phenoelit-us.org/stuff/FX_Phenoelit_25c3_Cisco_IOS.pdf).

*6 Published materials relating to Return Oriented Programming (http://www.blackhat.com/presentations/bh-usa-08/Shacham/BH_US_08_Shacham_Return_Oriented_Programming.pdf).

*7 Information related to Conficker and Downadup variants can be found at, for example, Microsoft Malware Protection Center “Centralized Information About The Conficker Worm” (http://blogs.technet.com/mmpc/archive/2009/01/22/centralized-information-about-the-conficker-worm.aspx).

*8 Regarding the prevention of malware infections via USB memory by disabling AutoRun: Technical Cyber Security Alert TA09-020A (http://www.us-cert.gov/cas/techalerts/TA09-020A.html); Microsoft (http://support.microsoft.com/kb/967715).

*9 For example, “Web alteration not relying on SQL or RFI” (http://jvnrss.ise.chuo-u.ac.jp/csn/index.cgi?p=SQL%A4%C8%A4%ABRFI%A4%F2%BB%C8%A4%EF%A4%CA%A4%A4Web%B2%FE%E3%E2). (in Japanese)

"Click-jacking" emerged last year as a malicious technique that involved the inducement of unexpected behavior from user clicking. A technical report*10 was released about this technique. Other incidents involved messages disguised as New Year's or Valentine's Day greetings, attempting to expose users to malware infections.

■Other

While not directly related to security, a defect*11 related to Seagate Technology hard drives received attention due to aspects involving availability. Elsewhere, several BGP implementations were affected operationally due to the distribution*12 of routing information having extremely long AS Path attributes. Networks that used these BGP implementations observed interruption or unstability of communications; however, there were no incidents that affected networks directly operated by IIJ.

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 of 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 JPCERT/CC Technical Notes "About Click-Jacking Defenses" (http://www.jpcert.or.jp/ed/2009/ed090001.pdf). (in Japanese)

*11 See the official Seagate Technology announcement (http://seagate.custkb.com/seagate/crm/selfservice/search.jsp?DocId=207931).

*12 See, for example, NANOG Mailing List Archive (http://www.merit.edu/mail.archives/nanog/msg15468.html).

Figure 2 shows the circumstances of DDoS attacks handled by the IIJ DDoS Defense Service between January 1 and March 31, 2009. This information shows traffic anomalies judged to be attacks based on IIJ DDoS Defense Service standards. IIJ also responds to attacks perpetrated on clients of other IIJ connection services; however, 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*13, attacks on servers*14, 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 197 DDoS attacks. This averages to two attacks per day, but represents a decline in average incidents compared to our prior report (September through December, 2008). No bandwidth capacity attacks were noted. Server attacks accounted for 94% of all incidents, and compound attacks accounted for the remaining 6%. The largest server attack was a SYN flood of 90,000pps—an attack of a scale that can seriously compromise a server; however, the maximum traffic volume was around 108Mbps, which was observed in compound attacks. As to the reason behind the infrequency and small scale of bandwidth attacks, we believe that such lies in the fact that an attacker is also affected by heavy traffic loads.

Of all attacks, 74% ended within 30 minutes of commencement, while the remaining 26% 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*15 and botnet*16 usage as a means for carrying out DDoS attacks.

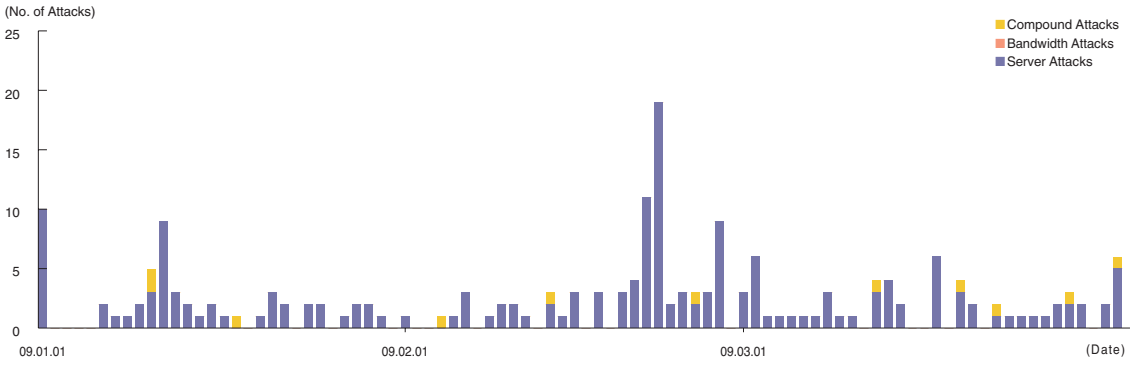


Figure 2: DDoS Attacks

*13 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.

*14 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 wasted consumption 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.

*15 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.

*16 A "bot" is a type of malware that institutes an attack after receiving a command from an infected 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)*17, malware activity observation project operated by IIJ. The MITF uses honeypots*18, 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 an attempt to locate a target for attack.

■Status of Random Communications

Figure 3 shows trends in the total volumes of communications coming into the honeypot (incoming packets) between January 1 and March 31, 2009. Figure 4 shows the distribution of sender's IP addresses by country.

The MITF conducts observations using numerous honeypots. Here, however, we have taken the average per honeypot, showing the trends for incoming packet types (top ten) over the entire period subject to study. Many are TCP ports used by the Microsoft OS, searching for clients. The MITF also observed searching behavior for 2967/TCP used by Symantec client software.

At the same time, the MITF observed 11075/UDP, 20689/UDP—communications not used by most applications—the goals of which were not clearly identifiable. Attacks on 445/TCP etc. targeting the MS08-067 vulnerability have continued since last October.

Looking at the overall sender distribution by country, we see that attacks sourced to Japan and China, 36.1% and 23%, respectively, were comparatively higher than the rest.

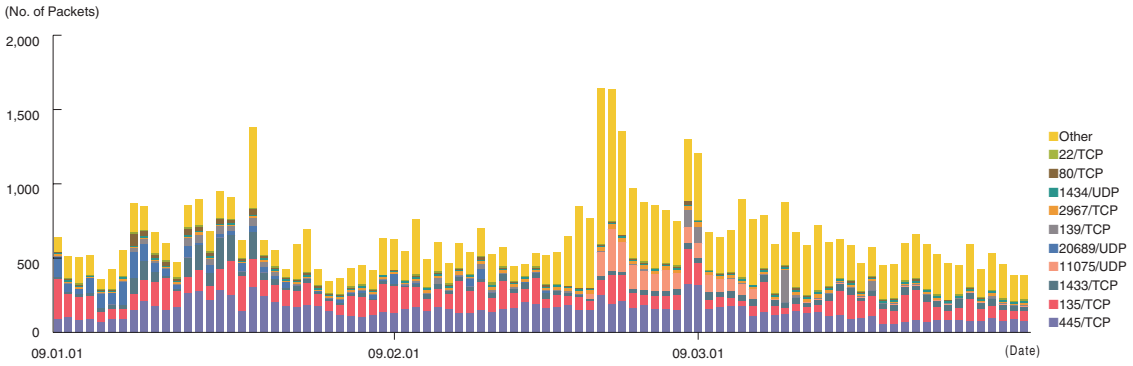


Figure 3: Communications Arriving at Honeypots (By Date, By Target Port, Per Honeypot)

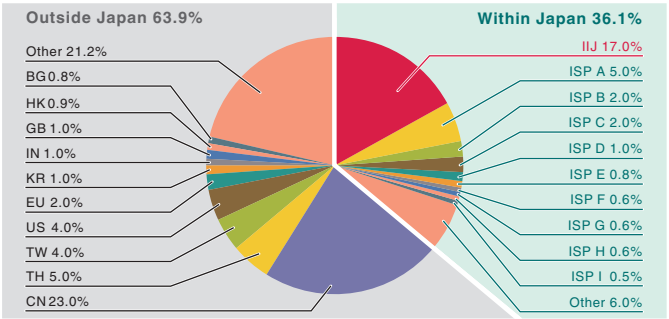


Figure 4: Sender Distribution (Entire Period under Study)

*17 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.

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

■Malware Network Activity

Next, let's take a look at the malware activity observed by the MITF. Figure 5 shows trends in the total number of malware specimens*19 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, while the number of unique specimens is the number of specimen variants categorized according to their hash values*20.

A total of 899 specimens were acquired per day on average during the period under study, representing about 44 different malware variants. According to prior statistics, the average daily total for acquired specimens was 2,235, with 55 different variants. Though we see a major 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 70.1%, with other countries accounting for the 29.9% balance. Of the total, malware infection activity among IIJ users was 33.0%. This shows that malware infection activity continues to be extremely localized.

The MITF prepares analytical environments for malware, conducting its own independent analyses of specimens acquired. The results of these analyses show that, during the period under observation, 14% of the malware specimens were worms, 45% were bots, and 41% were downloaders. In addition, the MITF confirmed the presence of 86 botnet C&C servers*21 and 540 malware distribution sites.

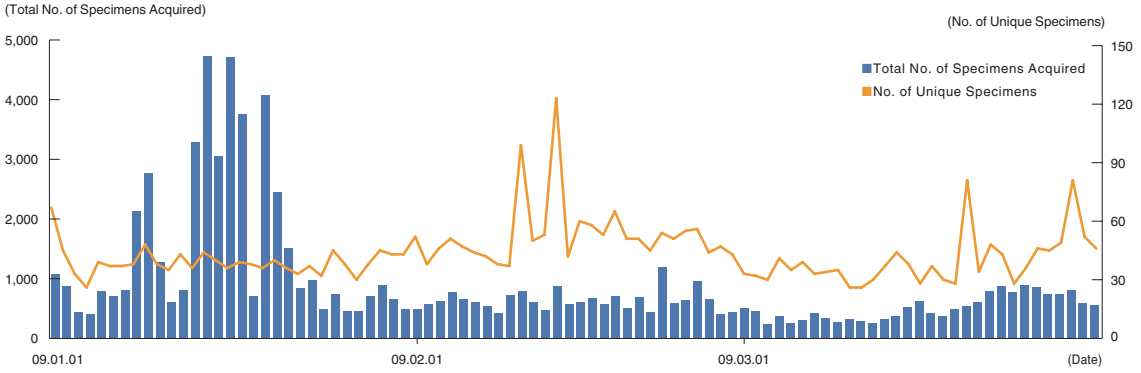


Figure 5: Trends in Number of Malware Specimens Acquired (Total Number, Number of Unique Specimens)

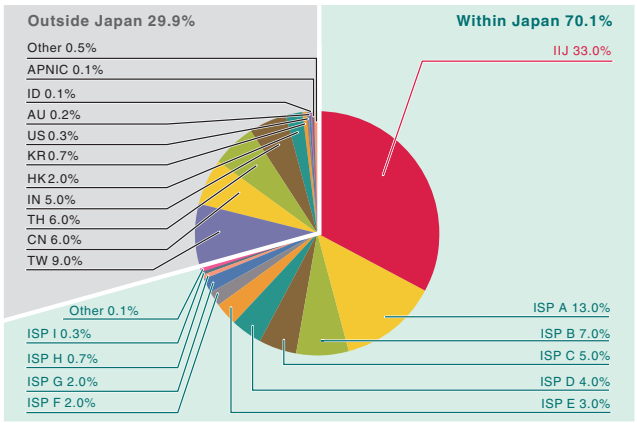


Figure 6: Distribution of Acquired Specimens by Source (Entire Period under Study)

*19 This indicates the malware acquired by honeypots.

*20 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.

*21 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*22. 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 delete or rewrite Web content, and those that attempt to gain full control over servers.

Figure 7 shows trends of the numbers of SQL injection attacks against Web servers detected between January 1 and March 31, 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. However, we have not included large scale attacks that have continued since the end of the prior year. Japan accounted as the source for 38.5% attacks, while South Korea and the United States represented 20.3% and 8.3%, respectively, with other countries accounting for the rest. As detailed in our previous report, there was a large-scale SQL injection attack against a few certain Web servers that began at the end of December 2008. These attacks dropped off rapidly beginning in 2009, quieting almost completely by the end of the first week of January.

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

See 1.4.1 “SQL Injection Attacks and their Impact” for more information about SQL injection attacks.

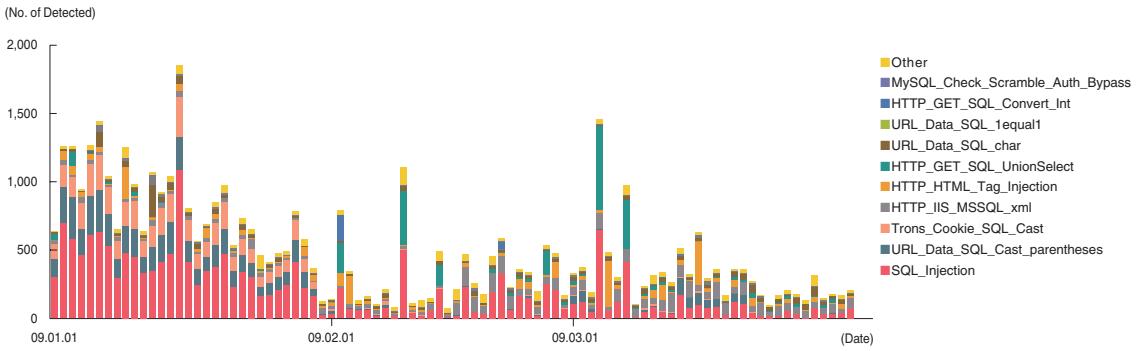


Figure 7: Trends of SQL Injection Attacks (By Day, By Attack Type)

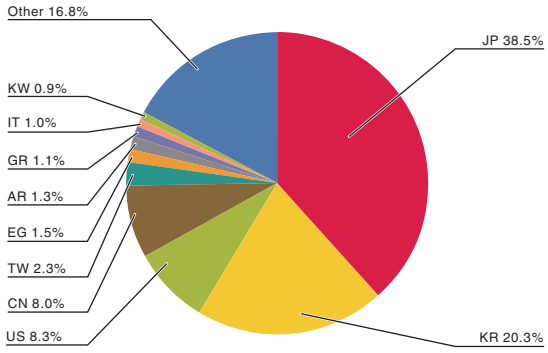


Figure 8: Distribution of SQL Injection Attacks by Source

*22 Attacks accessing a Web server to issue SQL commands, thereby connecting to and manipulating an underlying database. The database content can be accessed or altered without proper authorization; attackers can steal sensitive information, rewrite Web content, or otherwise issue system commands to control the database server.

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. In this section, we will discuss SQL injection attacks and their impact, alerts concerning ID/password management, and scareware from among surveys conducted during the period under study.

1.4.1 SQL Injection Attacks and their Impact

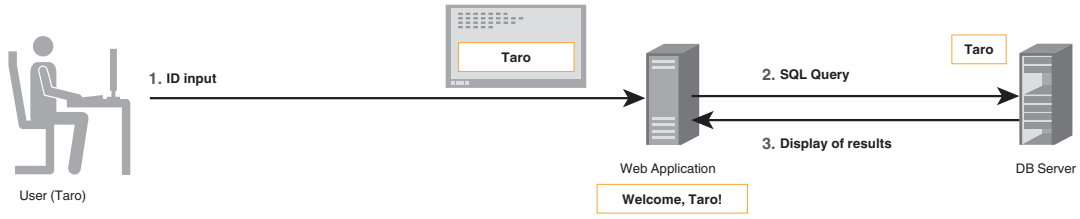
One method used to attack a Website is known as the SQL*23 injection attack. This type of attack uses remote requests to allow an attacker to perform unauthorized manipulation of a database (DB) used as a back end to a Website.

As discussed in "1.3.3 SQL Injection Attacks," this type of attack occurs continually on the Internet. As a result of this type of attack, customer information stored on a DB can be stolen, Web content can be altered to embed malicious programs or to lead users to malicious sites, etc., causing direct and real damage to users.

■Anatomy of a SQL Injection Attack

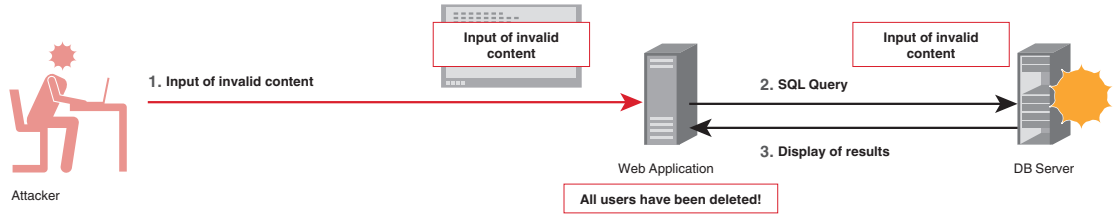
When a Web application makes an inquiry to a DB in response to a user request, a SQL statement is constructed for processing based on the user's input. If no special characters are included in the input value, the DB query is conducted as intended using the unmodified input values in the original SQL statement that serves as a template (Figure 9). However, if an attacker includes quotation marks or other special characters to create a text string that forms part of a SQL syntax, the SQL statement subsequently executed may result in different commands being sent to the DB than intended (Figure 10) if no input format checks or quotation mark escape characters are provided.

In this manner, a SQL statement different than the originally intended statement can be "injected," serving as a form of attack to cause behavior other than that desired. This is called a SQL injection attack. This attack can be implemented by various means, including via text input forms, or through Cookie HTTP header or GET/POST parameters, depending on Web application or DB implementations. These methods are used to slip through detection.



Under normal access conditions, user input is transmitted to a DB through a Web application, and the relevant content is produced.

Figure 9: Normal Processing



With a SQL injection attack, invalid input is transferred to a DB through the Web application, resulting in unintended behavior.

Figure 10: SQL Injection Attack

*23 SQL is a query language used to give commands to a database for data operations (search, insert, edit, delete, etc.).

In many cases, no error messages or other traces are left behind by the Web application or DB to give evidence of a completed SQL injection attack. This makes detection difficult under normal monitoring conditions. Given the nature of this kind of attack, many incidents are only discovered after a notification is received from a third party. This is particularly true in the case of unauthorized content alteration.

■Impact of SQL Injection Attacks

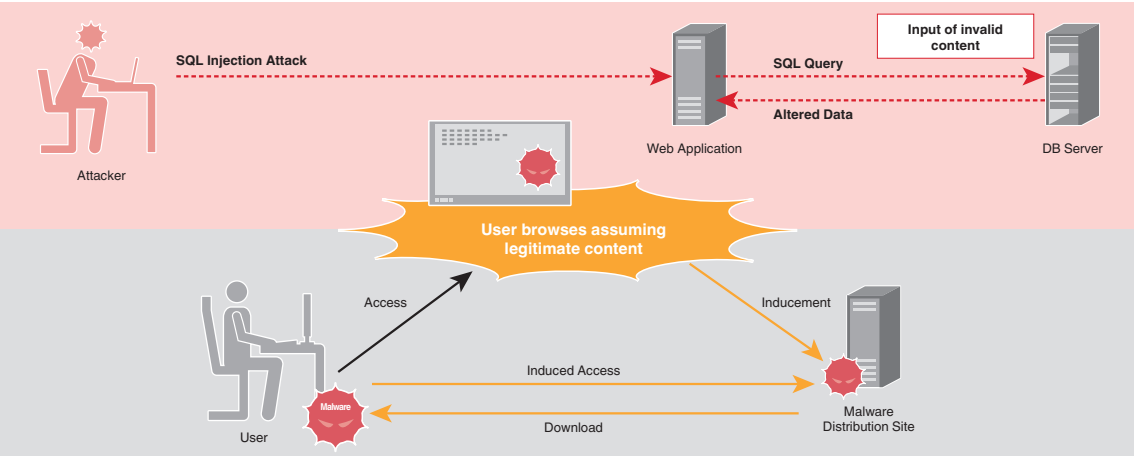
We can conceive of several different types of damages that can occur in the event of a successful SQL injection attack.

First, sensitive corporate or personal information stored in the database is at risk of theft or leakage. Second, attackers may delete or destroy data. Services over the Internet become impossible to provide if Web content and user information are deleted from service databases. Third, database content may be replaced with fraudulent content. If Web content is changed, an attacker can cause unintended information to be broadcast, leading visitors to malicious sites that cause malware infections, or other situations that present direct danger to the visitors. Fourth, a SQL injection attack can be the springboard for deeper systems penetration. An attacker may be able to set up a "back door" to control the system, using it as a stage to attack other systems across the network.

If left undetected or uncared for, successful SQL injection attacks can spread to cause significant damages to third parties and other systems.

■Attacking Users via Web Content Alteration

A recent increasing trend in SQL injection attacks is the alteration of Website content, and the installation of attack scripts that lead Website visitors to malware download sites*24 (Figure 11). Since the Web server itself is legitimate, users are not aware that the content has been changed, resulting in the greater likelihood of malware infection. In these situations, it is difficult for users to recognize the counterfeit information. It is important that Website operators take more active countermeasures against such threats.



Content alteration via SQL injection attack not only involves the alteration of Web server content; unsuspecting Website visitors may also be subject to harm.

Figure 11: Attacking Users via Content Alteration

*24 For example, "Threats to Systems Administrators and Developers No. 1 The Power of Attacks through Legitimate Websites" as detailed in "10 Major Security Threats (http://www.ipa.go.jp/security/vuln/10threats2009.html)" published by the Information Technology Promotion Agency, Japan. (in Japanese)

■Countermeasures

Last, we will offer a summary of measures that can be taken to prevent SQL injection attacks.

■ Care when Creating Web applications

When creating Web applications, Web developers must take care to design resistance to SQL injections. As mentioned previously, SQL injections are possible due to insufficient handling of invalid input text strings. First and foremost, developers can utilize a technique called a bind mechanism*25 when queries are made to the DB.

Other countermeasures include checking the format of text string input, limiting information contained in error messages to the smallest amount possible so as not to give away hints of vulnerabilities to attackers, and limiting access permissions to the DB appropriately. In addition, we also recommend that Web application operating tests include the use of software that tests Web application vulnerabilities, as well as the performance of third-party audits. For more detail, see the IPA's "How to Secure Your Web Site"*26 and the Open Web Application Security Project (OWASP) "SQL Injection"*27.

■ Operational Countermeasures

Today's websites are built using multiple software components; be sure to pay attention to information regarding implementation vulnerabilities. The same applies, even when providing static content only. To gain an accurate understanding of circumstances surrounding an attack, administrators must create an environment allowing for the recording/storage of communications logs (POST data, cookies, SQL query statements, etc.).

To detect irregularities in their early stages, and to establish an understanding of the circumstances surrounding an attack, systems should be designed and managed so DB query errors are flagged as alerts requiring administrator investigation. Systems owners can adopt IDS or IPS and WAF*28, or even look into hiring a managed security service provider.

1.4.2 Alerts Concerning ID/Password Management

■Unauthorized ID Usage Occurs All Too Frequently

According to a news story in September 2008, an identity fraud incident involving the theft of IDs and passwords victimized a Japanese auction Website. Many individuals were charged for commissions on items they had no recollection of selling. Reportedly, one of the root causes of this incident was that users were using the same ID and password combinations across a multiple number of Websites. Alerts were sent out warning users against using the same passwords for different Websites. Toward the end of 2008, incidents involving the unauthorized use of IDs to alter Website content began to grow significantly in number. Website visitors were subjected to malicious content causing them to be exposed to malware. IIJ confirmed some of the clients were numbered among the victims of such incidents.

*25 A bind mechanism is a function for safely handling text strings in a SQL statement that include special characters. By clearly separating the SQL statement syntax and the input values when creating text strings, Website developers can prevent the injection of invalid SQL statements.

*26 See "How to Secure Your Web Site" from the Information Technology Promotion Agency, Japan (http://www.ipa.go.jp/security/english/vuln/200806_websecurity_en.html).

*27 SQL injection countermeasures by OWASP (http://www.owasp.org/index.php/SQL_Injection).

*28 Web Application Firewall (WAF). A type of firewall that monitors Web communications, validating incoming input and outgoing content to prevent vulnerability exploits and unauthorized intrusions.

■Password Strength

Strong password selection methods and means for correctly managing passwords have been in existence for many years. An IPA alert*29 details basic management methods for requiring periodic password changes and login history confirmation. SANS Password Policy*30 and other best practices regarding strong password creation have been publicly available on the Internet, and there also have been open source software*31 that automatically creates strong passwords meeting certain requirements. Utilizing these methods introduces basic functions for ensuring a strong password for any given ID.

■The Difficulty of ID and Password Management

At the same time, Internet users now commonly make use of Internet shopping, SNS, blogs and other Web services. Many users use their email addresses as their IDs across a multiple number of Websites. Users are responsible for creating proper passwords on these Websites and exercising appropriate password management on their own. In other words, it is the Internet user who is in the position of having to create several different "strong passwords" at the various Websites whose services they frequent, periodically changing passwords for effective management. Of course, remembering so many different passwords is a difficult task, and users tend to "reuse" passwords among various Websites.

Given this situation, learning an ID and password at one service presents the potential for gaining fraudulent access to a multiple number of other services—a significant risk when sharing or allowing the disclosure of ID/password combinations.

■Recommendations for Users

Many users opt to have their Web browsers and email software "remember" their ID and password combinations. Several Web browsers incorporate built-in or add-on functions that let the user know which ID and password they are using at each site. We encourage users who are in the habit of using the same ID and password across a number of Websites to create new, different password for each site. Users should consider the impact of others finding out their ID/password combinations, and be sure to create unique ID and password combinations for different sites, particularly on important online services including online banking and online shops.

Next, consider using a method for remembering multiple passwords. For example, a unified password management tool (Password Safe*32, Password Wallet*33, etc.) can be used to access all of the passwords with a single master password.

■Recommendations for Administrators

From the standpoint of a corporate network administrator, the minimum for appropriate ID and password usage would be to train all members to not use their IDs or passwords at work for Websites of their personal use. While it isn't an easy matter to detect and identify cases in which an individual uses the same ID and password combinations for both work and personal use, the policy can be clearly stated within the organization, enhancing awareness by stressing the dangers of password "reusing" at work.

We recommend using systems that verify whether passwords being used on a corporate server can be easily guessed. In general, a method incorporating a dictionary*34 can be used.

*29 "Be sure to check your password(s) one more time!" from the Information Technology Promotion Agency, Japan (http://www.ipa.go.jp/security/txt/2008/10outline.html). (in Japanese)

*30 "SANS Password Policy" from the SANS Institute (http://www.sans.org/resources/policies/Password_Policy.pdf).

*31 For example, pwgen (http://sourceforge.net/projects/pwgen/).

*32 Password Safe (http://www.schneier.com/passsafe.html, http://passwordsafe.sourceforge.net/).

*33 Password Wallet (http://www.apple.com/downloads/macosx/productivity_tools/passwordwalletformacosxandiphone.html).

*34 For example, pam_cracklib, a LINUX PAM (Pluggable Authentication Module) that uses a dictionary to perform password checks (http://www.kernel.org/pub/linux/libs/pam/Linux-PAM-html/sag-pam_cracklib.html).

■Summary

Herein, we have identified several points about which users and administrators should be aware regarding the management of IDs and passwords. Are you using the same ID and password combinations without much thought for both servers at work and services that deal with private information (SNS, blogs, etc.) or one-time contest entry Websites? We highly recommend that readers perform an ID and password inventory.

1.4.3 Scareware

In this section, we will discuss the recently emerging threat of "scareware"—potentially malicious software pretending to be security software. Scareware is the name for a type of malware (a combination of the words "scare" and "software").

Scareware is software that acts as one component in a fraudulent scheme. When a user is browsing the Web, they are exposed to a message such as, "Your PC is infected by malware!" The effort is an attempt to fraudulently induce the user to purchase unnecessary software.

The following illustrates a typical scareware scheme, using the example of counterfeit anti-virus software:

1. When a user is browsing the Web, they are suddenly exposed to a pop-up message that reads, "Your computer might be infected with a virus. Do you want to check?" (Figure 12)

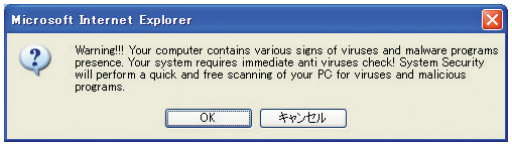


Figure 12: A Typical Scareware Pop-Up Message

2. Clicking the pop-up launches a screen that appears to be performing an online virus scan. (Figure 13)

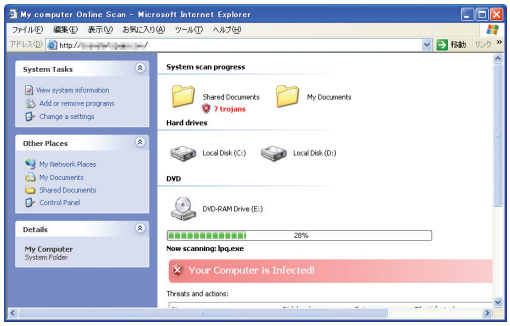


Figure 13: Fake Scan Screen

3. When the fake scan finishes, the user sees a pop-up screen such as the following: "Your computer is at risk. Immediately download and install anti-virus software." (Figure 14)

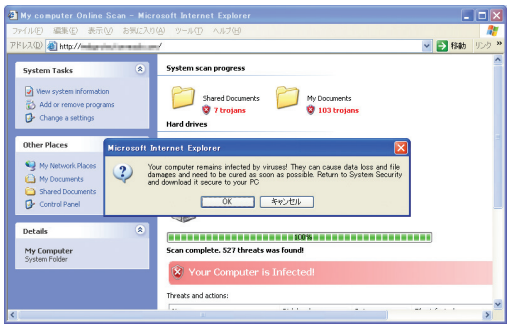


Figure 14: Fake Scan Results

4. If the user clicks the pop-up, they are taken to the fake anti-virus software vendor Web page (Figure 15), or at which point a direct download of the scareware begins.

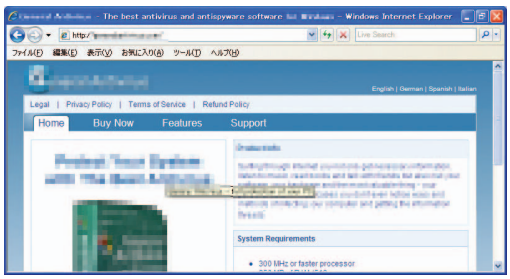


Figure 15: Example of a Fake Anti-Virus Software Vendor Web Page

5. The user downloads the fake anti-virus software, and installs it on their computer.

6. The fake anti-virus software will start automatically scanning the user's computer, falsely indicating that the PC is infected with numerous malware (Figure 16).

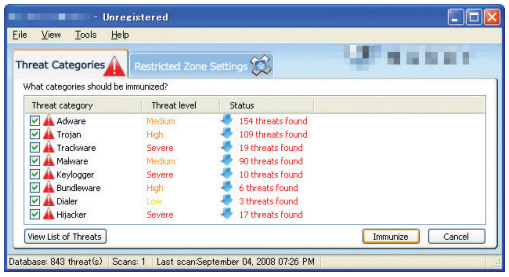


Figure 16: False Scan Results from Fake Anti-Virus Software

7. When the user clicks the button to remove the "detected" malware, they are instructed to buy a paid-for version of the software. This scheme convinces users that their computer is infected with malware, and they are then fraudulently induced to purchase worthless software (Figure 17).

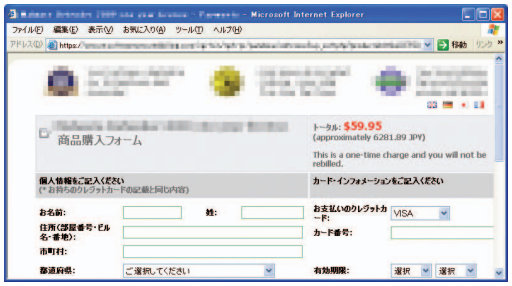


Figure 17: Example of a Fake Anti-Virus Software Purchase Screen

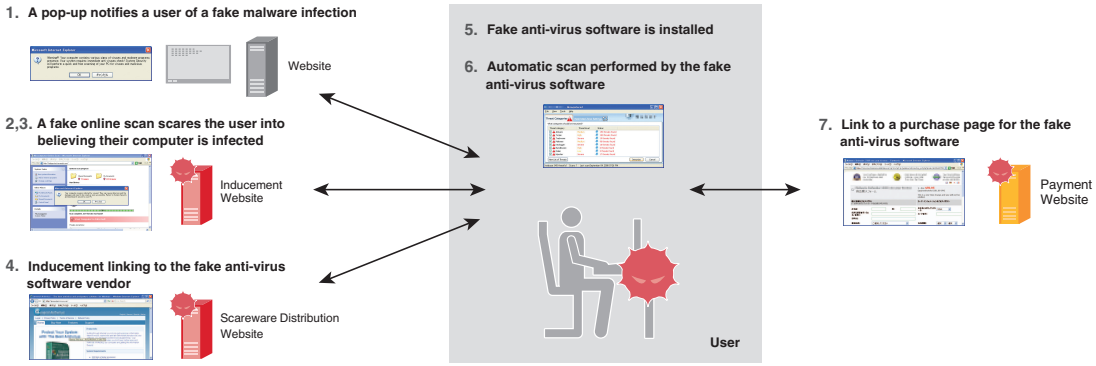


Figure 18: Anatomy of a Scareware Scam

In some cases, installed scareware will actually download and install malware on the pretext of an "update." The preceding chain of events is shown in Figure 18.

As shown in Figures 15 and 16, fraudulent anti-virus software vendor Web pages and screens have the same look and feel as those of legitimate software vendors, leading us to believe that the damages caused by this type of fraud will continue to spread. We have even come across cases of scareware written in Japanese.

In addition to the fake anti-virus software used above as an example, we have confirmed the existence of fake firewall and anti-spyware schemes as well. To avoid being scammed, it is important that users make a habit of using legitimate security measures software obtained from reputable vendors. For example, users can locate trustworthy anti-virus software by selecting products introduced by trusted information sources*35, or after confirming that a vendor is a member in good standing of an anti-virus industry association*36.

1.5 Conclusion

This whitepaper has provided a summary of security incidents to which IIJ has responded.

In addition to reporting on regular matters, this volume (Vol. 3) has also covered information related to password management and scareware, etc.—issues that are becoming more prevalent, and for which investigations and countermeasure development are ongoing. These incidents have yet to be resolved completely.

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 this important component of the social and corporate infrastructure.

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.

Shigeki Ohara, Hirohide Tsuchiya (1.4.1 SQL Injection Attacks and their Impact)
Tadaaki Nagao, Yuji Suga (1.4.2 Alerts Concerning ID/Password Management)
Hiroshi Suzuki, Takeshi Umezawa (1.4.3 Scareware)
Division of Emergency Response and Clearinghouse for Security Information, IIJ Service Business Department

Yasunari Momoi (1.4.1 SQL Injection Attacks and their Impact)
Service Promotion Section, Security Service Division, IIJ Network Service Department

Contributors:
Yoshinobu Matsuzaki
Technology Promotion Section, Network Service Division, IIJ Network Service Department

Kiyotaka Doumae
Planning Section, Data Center Business Planning and Operations Division, IIJ Service Business Department

*35 For example, products featured by ISPs, or products from vendors listed on Microsoft's Website (http://support.microsoft.com/kb/49500).

*36 Examples of anti-virus industry associations: VIA (Virus Information Alliance) (http://technet.microsoft.com/en-us/security/cc165596.aspx); AMTSO (Anti-Malware Testing Standards Organization) (http://www.amtso.org/members.html); ASC (Anti-Spyware Coalition) (http://www.antispywarecoalition.org/about/index.htm); etc.

2 Email Technical Report

2.1 Introduction

The Email Technical Report summarizes the latest trends in spam, technical counter measures to spam, etc. For trends in spam, the results of a variety of analyses conducted based on various information obtained from the Spam Filter feature provided in IIJ email services will be presented. Note that since the flow of email varies depending on the day of the week, in order to more easily understand the trends, the data was aggregated on a weekly basis using the week-numbering year*1 as the unit of data, and the data was analyzed focusing on the changes in the data.

This survey covers a period of 13 weeks or 91 days, from the first week of 2009 (12/29/2008 to 1/4/2009) to the 13th week (3/23/2009 to 3/29/2009).

Regarding technical counter measures to spam, continuing from the prior volume, “Sender Authentication Technologies” will be discussed. This volume will provide an overview regarding DKIM (DomainKeys Identified Mail) which uses digital signature technology.

2.2 Trends in Spam

This section provides a report focused on the trends in the ratio of spam detected by the Spam Filter feature provided by IIJ and information related to sources of spam. Regarding sources of spam, there has been a significant change since McColo’s network was shutdown in November 2008 (Reference: Internet Infrastructure Review Vol.2). Continuing from the prior volume, we will analyze these trends and changes.

2.2.1 Ratio of Spam

The weekly trends in the ratio of spam over a period of 91 days from the first week of 2009 to the 13th week are shown in Figure 1.

The ratio of spam averaged 81.5% of all incoming emails during this period. The ratio was highest during the first week (12/29/2008 to 1/4/2009) at 87.8%. This is because the period coincided with the year-end/new year holiday period and there was only a small amount of business email, thus the relative ratio of spam was higher. The average value for the prior period (9/1/2008 to 12/28/2008) was 82.7% and thus the ratio of spam decreased 1.2%. However, the ratio of spam is still very high and we believe it is necessary to continue to enhance spam control measures.

2.2.2 Sources of Spam

The sources of email that IIJ determined to be spam are listed by country in Figure 2.

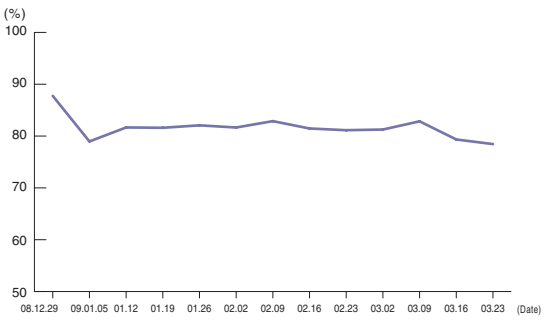


Figure 1: Ratio Proportion of Spam

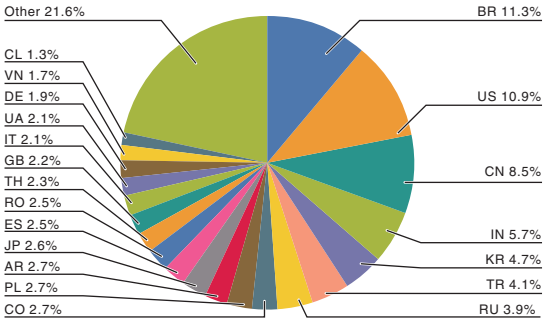


Figure 2: Sources of Spam

*1 Since the week-numbering year is determined based on ISO 8601 “Data Elements and Interchange Formats - Information Interchange - Representation of Dates and Times”, a period from 2008 is also included.

In this survey, the top source of spam was Brazil (BR) with 11.3%. This is a big jump compared to our prior survey. Brazil ranked only 5th with 5.5%. In the prior survey regarding the trends in sources of spam, Brazil ranked 2nd during the final week of 2008 (52nd week), thus there was a concern regarding the future increase in spam from this region.

The United States ranked 2nd (US, 10.9%) as in the prior survey, and China which ranked 1st in the prior survey ranked 3rd (CN, 8.5%). India ranked 4th (IN, 5.7%), which is a big jump from the prior survey when it ranked 8th. Korea (KR) ranked 5th, Turkey (TR) ranked 6th, and Russia (RU) ranked 7th, with all of three continuing to rank high in the list from the prior survey. Japan (JP) ranked 11th with 2.6%. According to this survey results, spam from Brazil, the U.S.A., and China made up approximately 30%, and spam from the top 7 countries made up approximately half of all spams. In order to reduce the amount of spam received in Japan, we believe it is necessary to implement control measures on the part of the sender, such as the implementation of OP25B*2 in these top ranking countries.

The weekly trends in the ratio of spam from these 7 countries and Japan are shown in Figure 3. U.S.'s ranking continued to fall after McColo's network was shutdown in November last year, but its ranking rose sharply from the 5th week (1/26 to 2/1) and thereafter it continued to rank high in the list. From this observation, we can presume that botnets which were previously affected by the shutdown of McColo's network have gained control over new management servers (Command & Control Servers), etc. and have resumed spamming activities. In addition, Brazil, whose ranking rose starting November of last year, continued to rank high in the list and as a result ranked no.1 for the entire period under study.

China, which ranked 1st in the prior survey, experienced a downward trend, however, its ranking rose again from the 12th week to the 13th week (3/16 to 3/29), requiring ongoing attention.

In the graph in Figure 3, we can see a difference in the trends in the ratio of spam sent from Japan and the ratio of spam sent from the other top ranking countries. Whereas the ratio of spam sent from Japan stayed relatively constant at approximately 2.5%, the ratio of spam sent from the other top ranking countries fluctuated considerably. This is an interesting difference and we plan to continue our research regarding the trends in the sources of spam and the differences in situations of each country which may have caused the fluctuation.

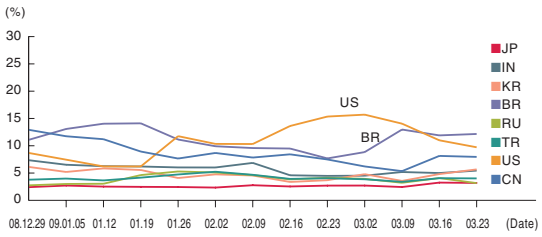


Figure 3: Trends in Sources of Spam

2.2.3 Spam Originating from Japan

As mentioned previously, in Japan, many ISP's have implemented OP25B, and thus it can be said that control measures against spam originating from Japan are relatively effective. The survey results for this report show that 97% or more of the spam was sent from outside Japan. Similar results were presented in a report created by Sophos Plc.*3, which periodically publishes a ranking of the top source countries of spam.

The results of "Communications Usage Trend Survey"*4 conducted by the Ministry of Internal Affairs and Communications in 2008 indicate that there are 90.91 million internet users in Japan, and that the proportion of broadband lines (FTTH, xDSL, CATV, etc.) used by households is 73.4%, indicating that the use of high-speed access lines is widespread. Although this condition alone would seem to suggest that in Japan there is a possibility for a massive amount of spam to be distributed over a short period of time, the results show that the actual amount of spam sent is low compared to other countries. We believe that this is due to the large number of ISP's implementing OP25B as well as the scale of implementation*5.

*2 OP25B (Outbound Port 25 Blocking) is technology that restricts access from dynamic IP addresses used by consumer users for internet connection to port number 25 which is used between mail servers in the external network, and it is known to be extremely effective in preventing spam from being sent.

*3 Sophos's URL is http://www.sophos.com/. In the 2008 spam source country ranking, Japan ranked 36th.

*4 Results of the survey conducted by the Ministry of Internal Affairs and Communications: http://www.soumu.go.jp/main_sosiki/joho_tsusin/eng/Releases/Telecommunications/news090407_b.html

*5 According to a study conducted by the Anti-Spam Consultation Center of the Japan Data Communication Association, 49 ISPs have implemented OP25B (http://www.dekyo.or.jp/soudan/common-folder/image/About_ASCC.pdf).

Although as a result of these efforts, the amount of spam originating from Japan has been reduced considerably, it is also a fact that this ratio has never reached zero. For example, the ratio of spam originating from Japan to the total amount of spam out of the total amount of email is equivalent to 2 emails for every 100 emails received. This figure is for the enterprise email service provided by IIJ, and thus in the case of mobile phone email, etc. the ratio may be even higher.

What are the sources of spam originating from Japan? One source may be spammers who have obtained a static IP address. Static IP address users are obviously not permitted to send spam, and in most cases, the sending of spam is considered improper use, and is grounds for termination of the contract with the ISP or the internet access service being used. However, it is very difficult for the administrator on the part of the sender to determine whether spam is being sent or not, and it is usually discovered after the recipient of spam makes a report, etc. In addition, it is necessary to find clear evidence that the person reporting the spam is providing correct information and that the contractee in question is actually sending spam, and it takes time to handle the problem.

Another source may unfortunately be the result of inadequate implementation of OP25B. It is known that spammers consistently target such loopholes and continue to send massive amounts of spam. One case that is recently becoming more common is where spam is sent using mobile data communications terminals. Mobile data communications are a convenient service which can be used anywhere, and the number of users has been rapidly increasing. However, at the same time, the misuse of these services is also becoming more common. There is a plan to implement OP25B, and since the effectiveness of OP25B has been confirmed, its implementation at an early stage is desirable.

In order to eliminate spam originating from Japan, it is necessary to correct these inadequacies on the part of the sender. In addition, learning from Japan's experience, to reduce the amount of outgoing spam at a global level, we believe it is important that OP25B be implemented in each country. IIJ presents the advantages of OP25B at various international conferences and opportunities, and we plan to continue to actively provide information.

2.3 Trends in Email Technologies

2.3.1 Trends in Sender Authentication Technologies

In the prior volume, we introduced two technologies for sender authentication: one is a network based technology, and the other is one that uses digital signature technology. Network-based SPF/Sender ID technology was covered in a series in the prior volumes, and in this volume we will provide an overview on DKIM (DomainKeys Identified Mail) which uses digital signature technology.

According to a study conducted by WIDE Project*6, the rate of publication of SPF records for “jp” domains in March 2009 was 34.77%, which is a 1.49% increase since the time of publication of the prior volume (January 2009). This was only a small increase compared to the previous increase (8.84%), but considering the fact that the number of domains is also increasing, it can be said that the number of domains implementing SPF is steadily increasing. In addition, for “co.jp” domains which are used by incorporated companies, the rate of publication of SPF records increased from the prior volume and reached a high 41.71%. In light of the harmful effects such as bounced email described in the prior volume, this trend indicates a growing awareness regarding the protection of domain names as corporate brands.

Meanwhile, the general rate of publication of DKIM-related records is 0.38%, indicating a substantial delay in implementation. This is said to be caused by the big difference in implementation cost on the part of the sender.

2.3.2 Sender Authentication Technologies Using Digital Signature Technology

The purpose of sender authentication technologies is to enable the receiving side to determine the authenticity of the sender information claimed in the incoming email. In other words, these technologies authenticate that the email is sent from a source that is approved by the administrator (domain) of the sender identified in the sender information.

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

In network-based SPF/Sender ID technology, the sender publishes the SPF record in the DNS. In DKIM, a digital signature which can only be appended by the sender managing the private key is appended to the email header. If the private key on the part of the sender is properly managed so that it is not leaked, it is generally difficult for a third party who doesn't know the private key to create a digital signature. This mechanism enables identification of the sender.

To implement DKIM on the part of the sender, in addition to the steps required for sending email, steps to create a digital signature using the email that is to be sent, and steps to append the signature to the email header need to be carried out. Since these steps are usually performed on the outgoing mail server, there is no impact on general email senders; however, new features need to be added to the outgoing mail server. The cost of adding these features is significantly higher than the cost of implementing SPF/Sender ID in which a record is simply published in the DNS one time, resulting in the substantial difference in penetration rate.

2.4 DKIM Authentication Flow

The DKIM specifications have been published as RFC4871 by IETF. The authentication flow for DKIM is shown in Figure 4.

```
DKIM-Signature: a=rsa-sha256; d=example.net; s=brisbane;
      c=simple; q=dns/txt; i=@eng.example.net;
      t=1117574938; x=1118006938;
      h=from:to:subject:date;
      z=From:foo@eng.example.net|To:joe@example.com|
      Subject:demo=20run|Date:July=205,=202005=203:44:08=20PM=20-0700;
      bh=MTIzNDU2Nzg5MDEyMzQ1Njc4OTAxMjM0NTY3ODkwMTI=;
      b=dzdVyOfAKCdLXdJOc9G2q8LoXSlEniSbav+yuU4zGeeruD00lszZ
      VoG4ZHRNiYzR
```

Figure 5: Example of DKIM-Signature

2.4.1 Sender Actions

The signature of the email is stored in the DKIM-Signature header field. The DKIM-Signature header field contains the signature itself and information such as the signed header fields, a hash, an encryption algorithm, query method for retrieve the public key, the expiration date of the signature, etc. which are set as parameters in the header.

First a hash value is calculated for the email body and email header respectively. Before calculating the hash values, the email body and email header are canonicalized to prepare them for the message modifications*7 carried out when the email is transmitted. The hash value for the email body is BASE64 encoded and stored as the "bh=" tag (parameter) in the DKIM-Signature header field. The DKIM-Signature header field is always included before calculating the hash value for the email header. The other email header fields to be included in the hash calculation (i.e. header fields to be included in the signature) are selected and the selected header field names are specified in the "h=" tag of the DKIM-Signature header field. At this stage, the final signature information is unknown, thus the "b=" tag which indicates the signature information in the DKIM-Signature header field is not included in the hash value calculation of the header*8. Since the hash information for the email body is included in the hash value calculation of the header, the email body is also included in the signature.

Signature information is created using public key cryptography technology based on the hash value of the header.

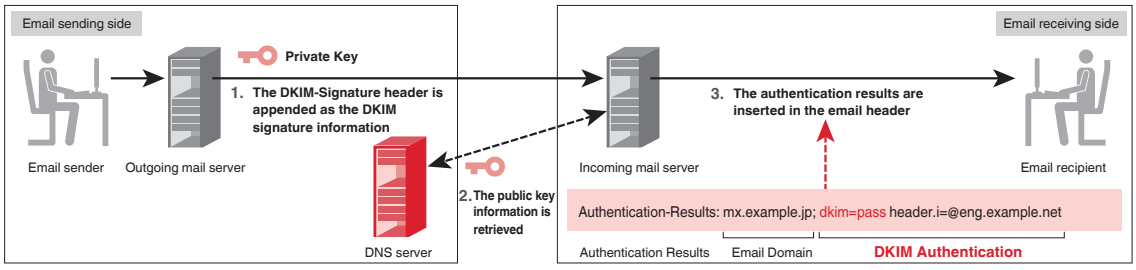


Figure 4: DKIM Authentication Flow

*7 For example, RFC5322 specifies a recommended value (98 characters or less) and a maximum value (998 characters or less) for the length of one line of an email body or header to be sent, and the mail server may automatically reformat the email by wrapping lines.

*8 The "b=" string, which indicates the parameter name, is included but the value after the "=" is set to blank before performing the calculation.

2.4.2 Process on the Receiving Side

The server receiving an email which contains DKIM signature information first retrieves the public key upon receiving the email. The retrieval method is specified in the "q=" tag of the DKIM-Signature header field but DNS is used by default. The domain name from which the public key is to be retrieved is constructed from the domain name specified in the "d=" tag of the DKIM-Signature header field and the selector specified in the "s=" tag. For example, in the header shown in Figure 5, the domain name is "example.net" and the selector is "brisbane." Thus the location shown in Figure 6 will be referenced.

```
brisbane._domainkey.example.net
```

Figure 6: Example of Public Key Retrieval Location

The sub domain "_domainkey" following the domain of the signing entity "example.net" is a fixed name under which the DKIM key information, etc. is stored.

As described above, the retrieval location of the public key cannot be determined until the actual email is received and the DKIM-Signature header field in the email is examined. This makes it difficult to conduct a study on DKIM implementation. On the other hand, there are also benefits to using selectors. Since DNS has a caching mechanism, even if a record is rewritten, the email receiving side is not immediately updated, and the timing of the update is also variable. By storing a new public key in a domain which uses a different selector, the selector name can be changed when the matching private key is changed, allowing the receiving side to retrieve the public key that corresponds to the signature without any confusion. In addition, by creating a sub domain, the management of the key can be outsourced. This is convenient when outsourcing email operations to hosting services, etc. After the public key is retrieved, the email body is canonicalized similarly to when the email was sent. A hash value is then calculated and the value is compared with the value of the "bh=" tag. The public key is used to verify the signature using the algorithm indicated in the "a=" tag.

2.5 Conclusion

This volume's survey results indicate that the amount of spam remains high at over 80% of all emails. As the sources of spam are rapidly changing it seems that spammers are aggressively seeking new methods for sending spam since the shutdown of McColo's network in November last year, and we believe that it is likely that the condition may worsen in the future. IIJ plans to continue to globally promote Japan's best practices in spam control such as implementing OP25B, etc. in order to support the reduction of spam. In addition, since there is still a certain amount of spam originating from Japan, we believe it is important to work on measures for patching the remaining loopholes on the part of the sender. In this volume, an overview on DKIM, a sender authentication technology using digital signature technology, and the DKIM implementation trends were presented. DKIM not only allows you to determine authenticity of the email sender, but it also allows you to determine whether the email contents have been altered, and it can be used to secure the reliability of email which is becoming an ever more important communication tool. IIJ plans to continue to promote the widespread use of these technologies and actively provide information in order to help ensure secure email connections.

Author:
Shuji Sakuraba
Shuji Sakuraba is a Senior Program Manager in the Service Promotion Section of the Messaging Service Division in IIJ Network Service Department. He is in charge of planning and researching email systems. He is involved in various activities in collaboration with the R&D department and 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.

Internet Topics: The 21st Annual FIRST Conference

■About FIRST

When dealing with incidents and problems occurring on the Internet, it is necessary to cooperate with many other organizations to take appropriate measures. Although incidents are becoming more localized nowadays, this cooperation is still very useful, because for instance, understanding incidents that have occurred in other countries enables us to prepare for future incidents. As an Internet service provider, IIJ participates in several international organizations to take part in such cooperation activities. Among such international organizations is FIRST*1.

FIRST was established in 1990 for the purpose of handling international incidents. In handling international incidents, what is necessary is the cooperation of people with various backgrounds, who are from different cultures, are subject to different laws, use different languages, live in various time zones, have different roles, etc. To make such international cooperation smooth and efficient, FIRST has several rules including those to keep confidentiality of sensitive information and to use English as the official language.

FIRST is an organization of CSIRTs*2 and consists of approximately 200 member teams from various organizations around the world, including CSIRT specialized organizations, national security agencies, universities, research institutes, commercial companies, etc.

■Annual FIRST Conference

FIRST conducts a wide variety of activities between members, from online discussion to face-to-face meetings. FIRST hosts several meetings per year, the largest of which is the Annual FIRST Conference. The Annual FIRST Conference has been held every June, in various cities throughout the world. While most of FIRST's activities are restricted only to members to maintain confidentiality of sensitive information, the Annual FIRST Conference is open to everyone who doesn't belong to a member team*3, and its participants count approximately 400 every year.

The Annual FIRST Conference for this year, will be held in Kyoto from June 28 to July 3*4, 2009. As of this writing, some part*5 of the program has been published and the call for participation is open.

The program covers a wide variety of topics including technical topics as also discussed in other information security conferences, as well as information on situations of the attacker's side, trends of international cooperation activities, introduction to schemes and case studies of cooperation between organizations of various types (such as national agencies, law-enforcement agencies, ISPs and product vendors), case studies of incident response based on actual experience of attacks, etc.

In addition, many of the participants as well as speakers are the foremost security professionals; The Conference offers a valuable opportunity of such experts from around the world gathering in Japan. We therefore urge you to participate in the 21st Annual FIRST Conference, and take full advantage of this opportunity to learn the latest trends and build cooperative relationships*6.

Author:
Mamoru Saito
Division of Emergency Response and Clearinghouse for Security Information, IIJ Service Business Department

*1 http://www.first.org/
*2 Computer Security Incident Response Team (CSIRT) is an expert group that handles incidents and problems in which computers are involved.
*3 During the Conference, there are also some meetings restricted only to members (such as the Annual General Meeting).
*4 http://conference.first.org/
*5 http://conference.first.org/program/program.aspx
*6 Please note that recording or taking pictures during the Conference is prohibited to keep confidentiality of anonymous presentation, mention of sensitive information and such.

Ongoing Innovation

About Internet Initiative Japan Inc. (IIJ)

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

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

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

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

IIJ-MKTG020AA-0906AK-01000PR