

Year 2010 Issues on Cryptographic Algorithms

In this report, we will explain incidents that occurred between April and June 2010, and also examine trends in the Year 2010 Issues on Cryptographic Algorithms, our observations on the backscatter caused by DDoS attacks, and trends in the vulnerability information circulation.

1.1 Introduction

This report summarizes incidents to which IIJ responded, based on general information obtained by IIJ itself related to the stable operation of the Internet, information from observations of incidents, information acquired through our services, and information obtained from companies and organizations with which IIJ has cooperative relationships. This volume covers the period of time from April 1 through June 30, 2010. In this period incidents of Gumblar and similar malware designed to steal IDs and passwords that we examined in previous reports continued to occur, along with cases of direct attacks on entities such as blog systems that led to content alteration and malware infections. There have also been a series of vulnerabilities discovered in Web browsers. Besides these incidents, targeted attacks were also conducted against specific countries and corporations. 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, 2010. Figure 1 shows the distribution of incidents handled during this period*1.

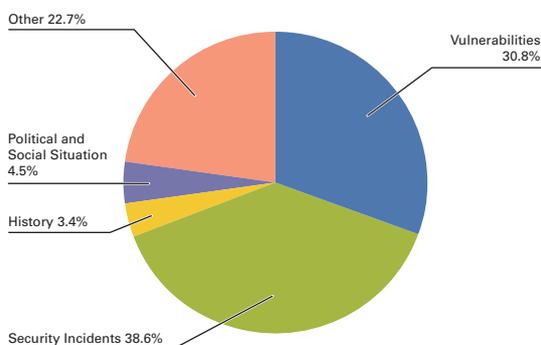


Figure 1: Incident Ratio by Category (April 1 to June 30, 2010)

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

■ Vulnerabilities

During this period a large number of vulnerabilities related to Web browsers and their plug-ins were discovered and fixed, including Microsoft's Internet Explorer*², Adobe Systems' Adobe Reader and Acrobat*^{3,4}, Adobe Flash Player*⁵, Adobe Shockwave Player*⁶, and the Adobe Download Manager*⁷ that is used for product updates, as well as Oracle's Java Deployment Toolkit*⁸. Fixes were also made to OS vulnerabilities in Windows XP and Windows Server 2003*⁹, and a number of vulnerabilities were also fixed in Mac OS X*^{10,11}. Regarding applications, a vulnerability was fixed in JustSystems Corporation's Ichitaro*¹². Several of these vulnerabilities were exploited before patches were released.

■ Political and Social Situations

IJ pays close attention to various political and social situations related to international affairs and current events. During the period under study we paid close attention to events such as the Soccer World Cup that was held from June, but we noted no related Internet attacks.

■ History

The period in question included several historically significant days on which incidents such as DDoS attacks and website alterations have occurred. For this reason, close attention was paid to political and social situations. However, IJ did not detect any direct attacks on IJ facilities or client networks.

■ Security Incidents

Unanticipated security incidents not related to political or social situations were discovered in the form of targeted attacks on Vietnamese Internet users*¹³ that led to the creation of a botnet*¹⁴. Additionally, there were reports of a spynet*¹⁵ thought to be monitoring a number of targets in India such as government agencies and corporations.

Regarding malware activity, Gumblar and incidents similar to it that have been occurring since last year continued to occur, and an increase in SSL communications of an unknown purpose caused by a bot-type malware known as Pushdo that is installed onto infected PCs has been confirmed*¹⁶. Furthermore, attacks on blog sites that use U.S. hosting services*^{17,18} became more active, affecting applications such as WordPress*¹⁹, and there were many

*2 Microsoft Security Bulletin MS10-035 - Critical: Cumulative Security Update for Internet Explorer (982381) (<http://www.microsoft.com/technet/security/bulletin/ms10-035.msp>).

*3 Security update available for Adobe Reader and Acrobat APSB10-09 (<http://www.adobe.com/support/security/bulletins/apsb10-09.html>).

*4 Security updates available for Adobe Reader and Acrobat APSB10-15 (<http://www.adobe.com/support/security/bulletins/apsb10-15.html>).

*5 Security update available for Adobe Flash Player APSB10-14 (<http://www.adobe.com/support/security/bulletins/apsb10-14.html>).

*6 Security update available for Shockwave Player APSB10-12 (<http://www.adobe.com/support/security/bulletins/apsb10-12.html>).

*7 Security updates available for Adobe Reader and Acrobat APSB10-02 (<http://www.adobe.com/support/security/bulletins/apsb10-02.html>).

*8 Oracle Corporation, "Java™ SE 6 Update Release Notes" (<http://www.oracle.com/technetwork/java/javase/6u20-142805.html>).

*9 Microsoft Security Advisory (2219475) Vulnerability in Windows Help and Support Center Could Allow Remote Code Execution (<http://www.microsoft.com/technet/security/advisory/2219475.msp>). At the time of writing, this was fixed in Microsoft Security Bulletin MS10-042 - Critical: Vulnerability in Help and Support Center Could Allow Remote Code Execution (2229593) (<http://www.microsoft.com/technet/security/bulletin/ms10-042.msp>).

*10 About the content of Security Update 2010-003 (<http://support.apple.com/kb/HT4131>).

*11 About the security content of Security Update 2010-004 / Mac OS X v10.6.4 (<http://support.apple.com/kb/ht4188>).

*12 JVN#98467259 Ichitaro series vulnerable to arbitrary code execution (<http://jvn.jp/en/jp/JVN98467259/index.html>).

*13 We also comment on targeted attacks in Vol.7 of this report, under "1.4.2 Targeted Attacks and Operation Aurora" (http://www.ij.ad.jp/en/development/iir/pdf/iir_vol07_EN.pdf). As there are no technological countermeasures for this type of attack, with long-term measures such as user education being required, they are also sometimes called an Advanced Persistent Threat (APT).

*14 Details can be found in the following Trend Micro blog post. "Malware Spoof an Adobe Update and VPSKeys" (<http://blog.trendmicro.com/malware-spoof-an-adobe-update-and-vpskeys/>).

*15 See the following Shadowserver Foundation announcement for details (<http://www.shadowserver.org/wiki/pmwiki.php/Calendar/20100406>). The following F-Secure blog post also commented on this report. "Shadows in the Cloud" (<http://www.f-secure.com/weblog/archives/00001927.html>).

*16 JPCERT/CC Alert 2010-04-28: Gumblar-related drive-by-download attacks infecting PCs with DDoS clients (<https://www.jpcert.or.jp/english/at/2010/at100011.txt>). The Nippon CSIRT Association has also observed and presented an overview on these botnet-related communications (<http://www.nca.gr.jp/2010/pushdo-ssl-ddos/>) (in Japanese).

*17 The following Network Solutions blog post warns users about the WordPress vulnerability. "Alert: WordPress Blog & Network Solutions" (<http://blog.networksolutions.com/2010/alert-wordpress-blog-network-solutions/>).

*18 The following Go Daddy blog post warns users about content alterations. "What's Up with Go Daddy, WordPress, PHP Exploits and Malware?" (<http://community.godaddy.com/godaddy/whats-up-with-go-daddy-wordpress-php-exploits-and-malware/>).

*19 WordPress is open source blog software (<http://wordpress.org/>).

incidents of malware infections caused through a large number of content alterations that led users to other malicious websites*20.

JPCERT/CC has also released an alert*21 regarding targeted attack emails using clever Japanese wording. IPA has also published a report*22 that summarizes the characteristics of targeted attacks along with their countermeasures.

■ Other

Regarding trends for other security-related incidents, in order to facilitate the implementation of DNSSEC*23 for which preparations are underway in Japan, TCR selection*24 for implementing signature protection for the root zone at the top of the DNS hierarchy was carried out (signature protection was implemented in July 2010). Additionally, a symposium was held ahead of the establishment of the Cloud Security Alliance (CSA) Japan Chapter*25, which is an association for evaluating security related to cloud computing.

1.3 Incident Survey

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

1.3.1 DDoS Attacks

Today, DDoS attacks on corporate servers are almost a daily occurrence. The methods involved in DDoS attacks vary widely. Generally, however, these attacks are not the type that utilize advanced knowledge such as that of vulnerabilities, but rather cause large volumes of unnecessary traffic to overwhelm network bandwidth or server processes for the purpose of hindering services. Figure 2 shows the circumstances of DDoS attacks handled by the IIJ DDoS Defense Service between April 1 and June 30, 2010.

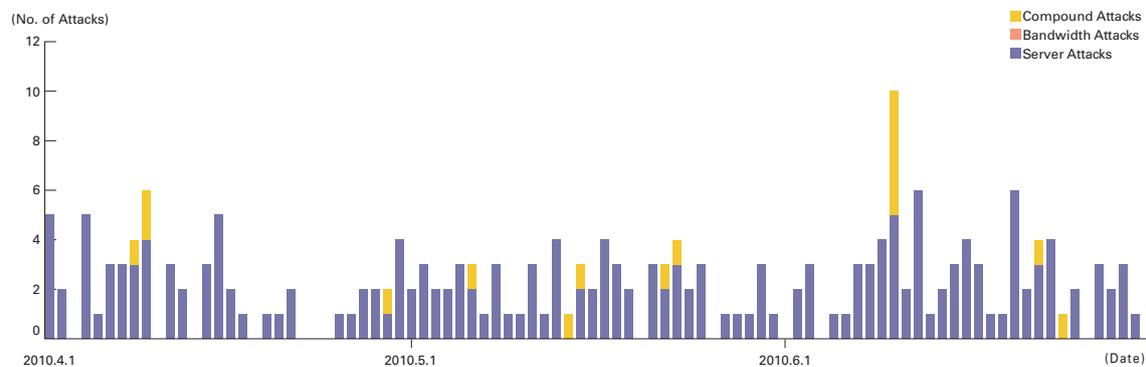


Figure 2: Trends in DDoS Attacks

*20 Details can be found in the following Trend Micro blog post. "WordPress Blogs Suffer from a Mass Compromise" (<http://blog.trendmicro.com/wordpress-blogs-suffer-mass-compromise/>).

*21 See JPCERT/CC Alert 2010-06-01: Emails purporting to advise of company internal malware outbreak contain malware (<http://www.jpcert.or.jp/english/at/2010/at100013.txt>) from the JPCERT Coordination Center.

*22 Tips for identifying irregularities and measures to take after an irregularity is identified based on actual examples of targeted attack emails - "Analysis and Countermeasures for Threats Targeting Vulnerabilities Vol.3" by IPA (Information-Technology Promotion Agency, Japan) (<http://www.ipa.go.jp/about/press/20100602.html>) (in Japanese).

*23 Details of trends related to DNSSEC implementation in Japan can be found in the following DNSSEC related information from JPRS (<http://jprs.co.jp/en/topics/2010/100728.html>).

*24 TCR (Trusted Community Representatives) are people who have the authority to generate and update the keys used for root DNS servers. With the implementation of signature protection for the root zone in July 2010, TCR were elected in June 2010 (<http://www.root-dnssec.org/tcr/selection-2010/>).

*25 Cloud Security Alliance Japan Chapter (<http://www.cloudsecurityalliance.jp/>).

This information shows traffic anomalies judged to be attacks based on IJ DDoS Defense Service standards. IJ 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 impact. Figure 2 categorizes DDoS attacks into three types: attacks on bandwidth capacity^{*26}, attacks on servers^{*27}, and compound attacks (several types of attacks on a single target conducted at the same time).

During the three months under study, IJ dealt with 205 DDoS attacks. This averages to 2.25 attacks per day, indicating that there was no significant change in the average daily number of attacks compared to our prior report. Bandwidth capacity attacks accounted for 0% of all incidents. Server attacks accounted for 92% of all incidents, and compound attacks accounted for the remaining 8%.

The largest attack observed during the period under study was classified as a server attack, and resulted in 160Mbps of bandwidth using about 40,000pps packets. Of all attacks, 92% ended within 30 minutes of commencement, while 8% lasted between 30 minutes and 24 hours. During the time period under study, IJ 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^{*28} and botnet^{*29} usage as the method for conducting DDoS attacks.

*26 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.

*27 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.

*28 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.

*29 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)*³⁰, a malware activity observation project operated by IJ. The MITF uses honeypots*³¹ 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, 2010. Figure 4 shows the distribution of sender's IP addresses by country. The MITF has set up numerous honeypots for the purpose of observation. We have taken the average per honeypot, showing the trends for incoming packet types (top ten) over the entire period subject to study.

Much of the communications arriving at the honeypots demonstrated scanning behavior targeting TCP ports utilized by Microsoft operating systems. As with the statistics for the previous period, we observed scanning behavior for 2967/TCP used by Symantec client software and 22/TCP used for SSH. At the same time, communications for which the goal was not clearly identifiable, such as 25162/TCP, 10263/TCP, and 15636/TCP (not used by widely used applications), were also observed.

Looking at the overall sender distribution by country, we see that attacks sourced to China at 21.1%, Japan at 19.4%, and Taiwan at 7.0% were comparatively higher than the rest.

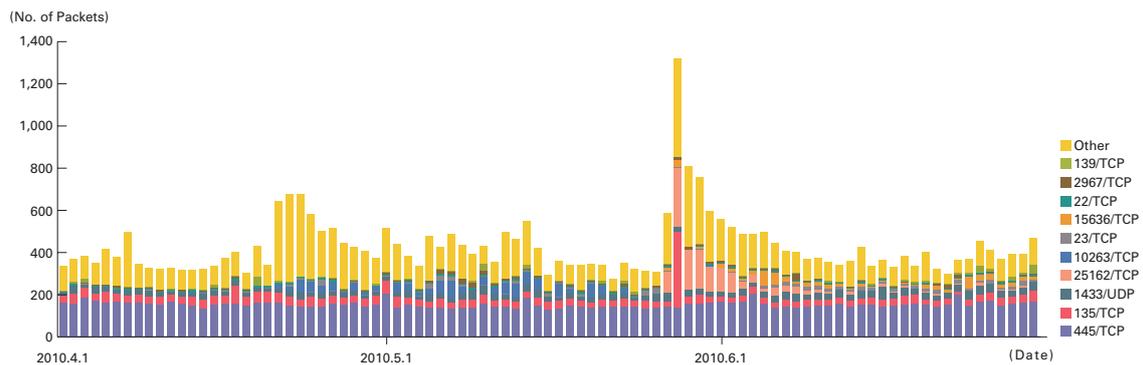


Figure 3: Communications Arriving at Honeypots (by Date, by Target Port, per Honeypot)

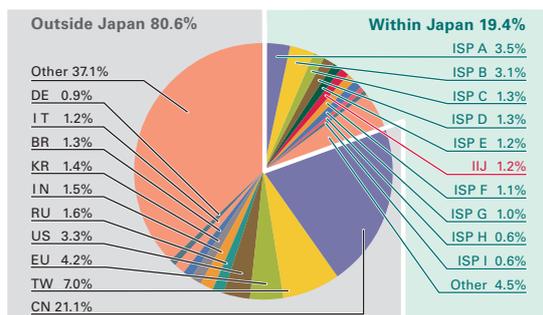


Figure 4: Sender Distribution (by Country, Entire Period under Study)

*³⁰ The Malware Investigation Task Force (MITF) began activities in May 2007 observing malware network activity through the use of honeypots in an attempt to understand the state of malware activities, to gather technical information for countermeasures, and to link these findings to actual countermeasures. See "1.4.3 MITF Anti-Malware Activities" in Vol.7 of the report for more details (http://www.ij.ad.jp/en/development/iir/pdf/iir_vol07_EN.pdf).

*³¹ 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, 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. In Figure 5, the trends in the number of acquired specimens show the total number of specimens acquired per day*³², while the number of unique specimens is the number of specimen variants categorized according to their digest of a hash function*³³.

On average, 378 specimens were acquired per day during the period under study, representing 32 different malware variants. According to the statistics in our prior report, the average daily total for acquired specimens was 479, with 37 different variants. For this period both the total specimens acquired and the number of different variants declined compared to the previous period.

The distribution of specimens according to source country has Japan at 49.6%, with other countries accounting for the 50.4% balance. Of the total, malware infection activity among IJ users was 0.1%, maintaining a low value similar to the previous period. Taiwan was at 28.9%, continuing to make up a large percentage as was the case for the previous report, and this is thought to be due to the increased activity of Sdbot and its variants in Taiwan.

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, 16.8% of the malware specimens were worms, 73.3% were bots, and 9.9% were downloaders. In addition, the MITF confirmed the presence of 27 botnet C&C servers*³⁴ and 4 malware distribution sites. The decrease in the number of malware distribution sites detected is due to the reduced number of downloader-type specimens obtained, and the drop in the number of specimens that access multiple distribution sites that were seen in the past.

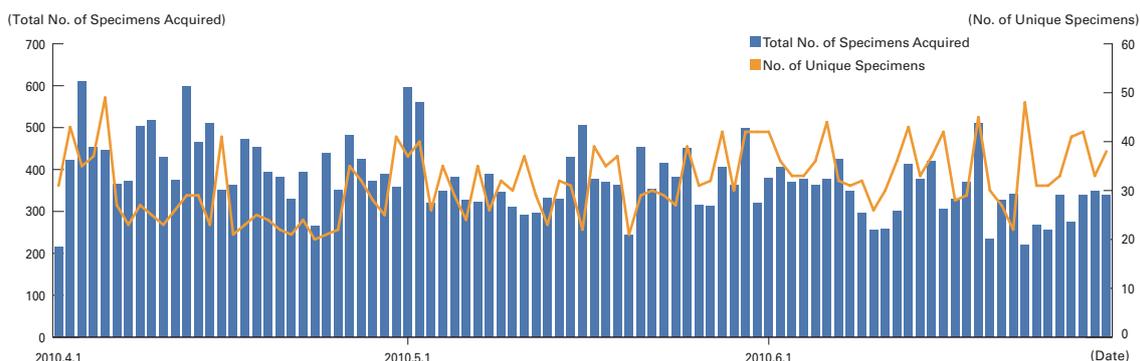


Figure 5: Trends in the Number of Malware Specimens Acquired (Total Number, Number of Unique Specimens)

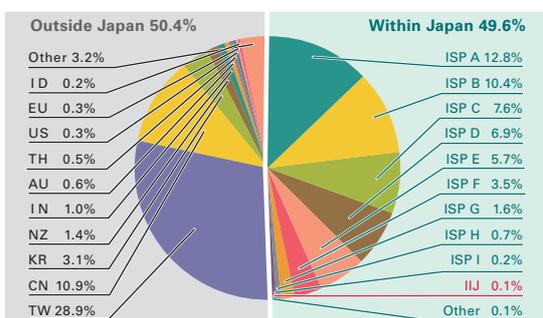


Figure 6: Distribution of Acquired Specimens by Source (by Country, Entire Period under Study)

*³² This indicates the malware acquired by honeypots.

*³³ This figure is derived by utilizing a one-way function (hash function) that outputs a fixed-length value for various input. The hash function is designed to produce as many different outputs as possible for different inputs. While we cannot guarantee the uniqueness of specimens by hash value, given that obfuscation and padding may result in specimens of the same malware having different hash values, the MITF has expended its best efforts to take this fact into consideration when using this methodology as a measurement index.

*³⁴ An abbreviation of "Command & Control." A server that provides commands to a botnet consisting of a large number of bots.

1.3.3 SQL Injection Attacks

Of the types of different Web server attacks, IIJ conducts ongoing surveys related to SQL injection attacks*35. 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, 2010. Figure 8 shows the distribution of attacks according to source. These are a summary of attacks detected by signatures on the IIJ Managed IPS Service.

Japan was the source for 31.3% of attacks observed, while China and the United States accounted for 24.7% and 11.8%, respectively, with other countries following in order.

We noted a greatly increased number of SQL injection attacks against Web servers during the current period. This is due to an increase in attacks against a specific small number of Web servers from overseas locations such as China and the United States. The number of attacks from within Japan was similar to the previous report.

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

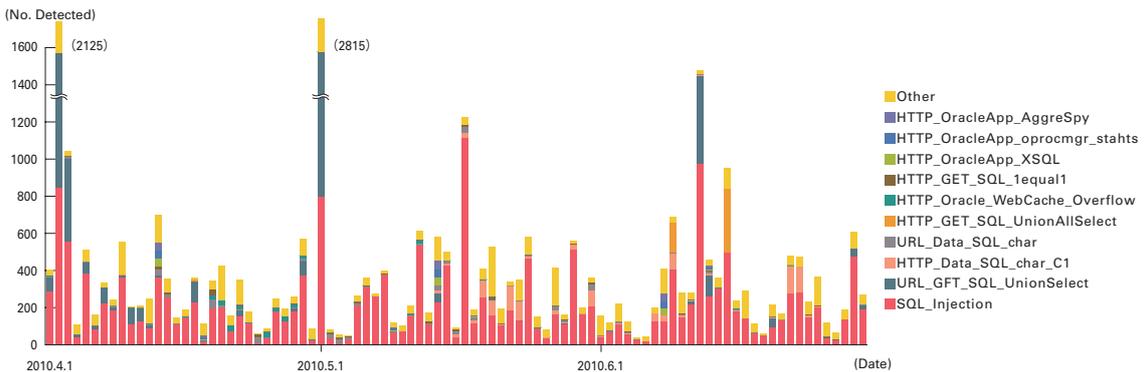


Figure 7: Trends in SQL Injection Attacks (by Day, by Attack Type)

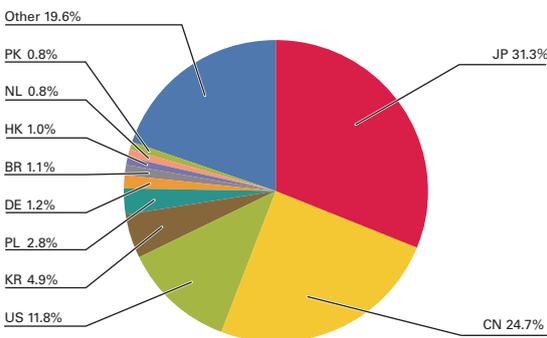


Figure 8: Distribution of SQL Injection Attacks by Source (by Country, Entire Period under Study)

*35 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 trends in the Year 2010 Issues on Cryptographic Algorithms, our observations on the backscatter caused by DDoS attacks, and trends in the vulnerability information circulation.

1.4.1 Trends in the Year 2010 Issues on Cryptographic Algorithms

In many ways the Year 2010 Issues on Cryptographic Algorithms can no longer be ignored, starting with the announcement from the National Institute of Standards and Technology (NIST)^{*36} that they will transition to next-generation cryptographic algorithms^{*37}. This originated from the attacks against multiple cryptographic hash functions^{*38} by researchers such as Joux and Wang at CRYPTO 2004. After hearing this announcement, the NIST issued a statement saying that the U.S. government would discontinue its use of SHA-1 by the end of 2010, and the issues relating to this deadline became widely known as the Year 2010 Issues on Cryptographic Algorithms^{*39}. Following this a schedule for the transition of cryptographic algorithms other than SHA-1 was also detailed, and it was indicated that in the future a number of algorithms will no longer be usable (NIST's Policy on Hash Functions^{*40}, and SP800-57^{*41}). Here, we examine why NIST decided to transition to other cryptographic algorithms, and look at the impact of this transition.

■ The Compromise of Cryptographic Algorithms

When the security properties of a cryptographic algorithm are jeopardized at a lower cost than expected when it was first designed, it is referred to as "compromised"^{*42}. Here, these security properties refer to the property of making it possible to decrypt plain text in symmetric key cryptography and public key cryptography only when in possession of the private key, and the property of making it hard to guess the private key from a set of plain text and encrypted text or the public key. For hash functions, these correspond to onewayness (the property of making it hard to find the source data from data that has been hashed) and collision resistance (the property of making it hard to find two different pieces of source data that are identical after hashing).

One of the primary factors behind a cryptographic algorithm being compromised is the improved analytical capability associated with increases in CPU processing power. From an attacker's perspective, an increase in processing power means that improved computational capacity is available for defeating encryption at the same cost as previous hardware. It is a fact that high performance hardware can now be obtained at affordable prices. For example, a cluster of PlayStation 3 consoles were used to search for MD5 collisions when making a counterfeit intermediary CA certificate^{*43}. Furthermore, environments that make it easy to access enormous computational power with little to no initial cost are developing rapidly, such as cloud services that will be readily available and purchasable for set periods of time without the need to set up any hardware.

Meanwhile, there are also cases where advancements in cryptanalysis research lead to compromises. The trouble with cases such as this is cryptographic algorithms that are currently in use may be compromised suddenly without warning. One possible countermeasure for this is the use of multiple algorithms with different mathematical backgrounds. Actually, some Web browsers implementing SSL/TLS contain multiple algorithms, with users able to select the algorithms to use^{*44}.

*36 National Institute of Standards and Technology (<http://www.nist.gov/>). An agency of the U.S. Department of Commerce that plays a central role in cryptography policy.

*37 NIST Brief Comments on Recent Cryptanalytic Attacks on Secure Hashing Functions and the Continued Security Provided by SHA-1, August 25, 2004 (http://csrc.nist.gov/groups/ST/toolkit/documents/shs/hash_standards_comments.pdf).

*38 Details can be found in the following paper: Arjen K. Lenstra, "Further progress in hashing cryptanalysis" (<http://www.marcomattiucci.it/hash.pdf>).

*39 Une and Kanda, "Year 2010 Issues on Cryptographic Algorithms", Institute for Monetary and Economic Studies, Bank of Japan, Discussion Paper No. 2006-E-8 (<http://www.imes.boj.or.jp/english/publication/edps/2006/06-E-08.pdf>).

*40 NIST's Policy on Hash Functions, March 15, 2006 (<http://csrc.nist.gov/groups/ST/hash/policy.html>).

*41 NIST Special Publication 800-57 "Recommendation for Key Management - Part 1: General" (http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf).

*42 IPA, Research Report "Regarding the Compromise of Cryptographs" (http://www.ipa.go.jp/security/fy16/reports/crypt_compromise/documents/crypt_compromise.pdf) (in Japanese).

*43 MD5 considered harmful today (<http://www.win.tue.nl/hashclash/rogue-ca/>).

*44 When using the Opera Web browser (<http://www.opera.com/>) it is possible to list and select the algorithms used for secure communications under Advanced > Security > Security Protocols > Details.

■ Describing the Deterioration of Security

A concept called “n-bits of security” is used as a measurement index to gauge how far the compromise of a cryptographic algorithm has progressed. When 2^n (2 to the n-th power) of computational effort is required to attack a cryptographic algorithm^{*45}, the corresponding algorithm is noted as having “n-bits of security.” In other words, for a given cryptographic algorithm, the actual computational effort required to jeopardize the security properties of that algorithm describes its state of compromise. In symmetric key cryptography, the theoretical value for the computational effort required for an attack is 2^n for the key space size when performing a brute force attack (n is the key length in bits). For hash functions, the values are 2^n for onewayness, and $2^{(n/2)}$ for collision resistance (n is the output bit length).

Triple DES is an example of a cryptographic algorithm which no longer offers the level of security it was once expected to have due to advancements in cryptanalysis research, which we indicated as the second primary factor in the compromise of algorithms. The key lengths of 2-key Triple DES and 3-key Triple DES are 112 bits and 168 bits respectively. This means that the theoretical values for their n-bits of security are 112 bits and 168 bits. However, as a result of cryptanalysis research, their compromise has progressed to 80 bit and 112 bit levels (see the above-referenced SP800-57). Hash function examples include MD5, which has an output length of 128 bits, but just 123.4 bits of security (theoretical value: 128 bits of security) for onewayness^{*46}, and SHA-1, which has an output length of 160 bits, but just 63 bits of security (theoretical value: 80 bits of security) for collision resistance^{*47}.

The method of describing algorithms as having n-bits of security has also been attempted for public key cryptography, with mapping carried out based on key length. For example, evaluations of RSA cryptography were presented by Lenstra et al. in 1999^{*48}, and by RSA Laboratories in 2000^{*49}. There were differences between these two evaluations, but in a reevaluation by Lenstra et al. in 2004^{*50}, an evaluation by NIST in 2007 (the above-referenced SP800-57), and an ECRYPT2^{*51} evaluation^{*52} which was last published in 2010, figures thought to be intermediate and adequate were presented. For example, the RSA cryptography key lengths corresponding to 80 bits of security for symmetric key cryptography were 1329 (Lenstra), 1024 (NIST), and 1248 (ECRYPT2) (Table 1). From a reverse perspective, RSA-1024 was judged to be equivalent to 80 bits of security by NIST, but only recognized as having 73 bits of security in ECRYPT2.

Meanwhile, reports from both NIST and ECRYPT2 presented an identical evaluation of elliptic curve cryptography (ECC), showing it as having n/2 bits of security with a key length of n bits. However, in an evaluation by Fujitsu in January 2010^{*53} it was given a higher evaluation than those from NIST and others, as shown in Table 2.

Table 1: Security Evaluations of RSA Key Lengths

n-bits of Security	Lenstra (1999)	RSA Lab (2000)	Lenstra (2004)	NIST (2007)	ECRYPT2 (2010)	FUJITSU (2010)
56		430			640	
64	682		640		816	850
80	1513	760	1329	1024	1248	1219
112	4509		3154	2048	2432	2206
128	6669	1620	4440	3072	3248	2832
192				7680	7936	6281
256				15360	15424	11393

Table 2: Security Evaluations of ECC Key Lengths

n-bits of Security	NIST/ECRYPT2	FUJITSU
64	128	122
80	160	152
112	224	214
128	256	245
192	384	371
256	512	497

*45 One type of conventional attack used on symmetric key cryptography involves brute force attacks in which symmetric key candidates are checked one-by-one to identify the key. Meanwhile, when a deficiency has been discovered in the characteristic structure of a cryptographic algorithm, efficient attacks that require less computational effort than brute force attacks are used. The security of public key cryptography is founded on mathematical difficulty. For example, in the case of RSA, private keys can be determined if the prime factorization of composite numbers is possible, so efficient prime factorization methods are used in attacks.

*46 Yu Sasaki, Kazumaro Aoki, “Finding Preimages in Full MD5 Faster Than Exhaustive Search”, EUROCRYPT2009 (<http://www.springerlink.com/content/d7pm142n58853467/>).

*47 RSA Laboratories, “SHA1 Collisions can be Found in 2^{63} Operations” (<http://www.rsa.com/rsalabs/node.asp?id=2927>).

*48 Arjen K. Lenstra, Eric R. Verheul, “Selecting Cryptographic Key Sizes” (<http://www.win.tue.nl/~klenstra/key.pdf>).

*49 A Cost-Based Security Analysis of Symmetric and Asymmetric Key Lengths, RSA Laboratories’ Bulletin #13 (<http://www.rsa.com/rsalabs/node.asp?id=2088>).

*50 Arjen K. Lenstra, “Key Lengths” (Contribution to The Handbook of Information Security) (<http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.90.213>).

*51 European Network of Excellence in Cryptology II. A cryptography-related research project to be carried out between August 2008 and July 2012, and one of the projects for the European Commission’s FP7 (Seventh Framework Programme) plan categorized under Information and Communications Technology (ICT) (<http://cordis.europa.eu/fp7/ict/>).

*52 ECRYPT II yearly report on algorithms and key sizes (2009-2010), EU FP7, ICT-2007-216676 (<http://www.ecrypt.eu.org/documents/D.SPA.13.pdf>).

*53 Fujitsu Laboratories, “Security Comparison of Elliptic Curve Cryptography and RSA” (<http://jp.fujitsu.com/group/labs/techinfo/technote/crypto/cryptanalysis.html>) (in Japanese).

Using this measurement index for compromise, the greater the value of n , the more that security is increased. In other words, by using longer key lengths for symmetric key cryptography and public key cryptography, and by increasing the output bit length of hash functions, it is possible to ensure a higher n value. However, because increasing the key length or output bit length generally causes cryptographic processing to take longer, it is necessary to select the algorithm and key length to use after considering computer processing load and user convenience.

■ Attitudes toward Algorithm Transition

Using the evaluation results presented on the previous page, it is possible to identify the relevant n -bits of security by setting conditions such as algorithm and key length. The question is, what value should the “ n ” in n -bits of security be? Here, we examine the attitudes and transition schedules of a number of countries.

First we will look at the U.S. government’s transition schedule. Table 4 in NIST’s SP800-57 that we mentioned previously shows a number of recommended algorithms and their corresponding minimum key sizes. According to this table, which was published in 2007, we can see that there is a transition from algorithms with 80 bits of security to algorithms with 112 bits of security by the end of 2010. Specifically, this indicates a schedule that phases out algorithms such as RSA-1024 and SHA-1 and fully transitions to algorithms such as RSA-2048 and the SHA-2 family^{*54} from the start of 2011. Furthermore, it is recommended that a minimum of 128 bits of security be secured by the end of 2030, with the schedule showing use of Triple DES is to be phased out in favor of a full transition to AES.

Preparations were being made based on this schedule until the first half of 2010, but in June 2010 NIST published a draft of the new SP800-131^{*55}. This draft presents a clearer transition schedule than SP800-57 drawn up in 2007. Instead of a full transition by the end of 2010, a grace period of three years (five years for 2-key Triple DES) has been established, with use expected to be possible until 2013 under a “Deprecated” status. This status indicates that use is only possible if the user accepts some risk.

Next, we will look at developments in European countries. In 2003 the NESSIE^{*56} project established a list of recommended cryptographic algorithms^{*57}. Here, the only mention of key length is for elliptic curve cryptography, and factors such as a time limit are not touched upon.

The transition policy published by Germany’s BSI (Bundesamt für Sicherheit in der Informationstechnik, Federal Office for Information Security)^{*58} covers the following hash function transitions. SHA-1 and RIPEMD-160, which have a theoretical value of 80 bits of security, will no longer be recommended after 2010, and after granting a grace period until 2015 (with use restricted to certificate validation), SHA-256 or higher SHA-2 family hash functions with a theoretical value of 128 bits of security will be recommended from 2016. Regarding RSA, 1728 bit key lengths are recommended until 2010, with key lengths of at least 1976 bits recommended from 2011 onwards.

The transition policy of France’s FNISA (French Network and Information Security Agency)^{*59} allows the use of symmetric key cryptography and hash function algorithms with 100 bits of security and RSA-2048 between 2010 and 2020, with transition to algorithms with 128 bits of security and RSA-4096 recommended from 2020 and beyond.

*54 SHA-224/256/384/512 are referred to collectively as the SHA-2 family. The numeric value associated with the algorithm name indicates the output bit length of the digest for each. Currently, NIST is holding a competition for the next-generation SHA-3 hash function. NIST, “Cryptographic Hash Algorithm Competition” (<http://csrc.nist.gov/groups/ST/hash/sha-3/>). The competition is now in the round 2 phase, with 14 algorithms remaining as candidates, and a final decision is expected to be made around the second quarter of 2012.

*55 Second Draft Special Publication 800-131, “Recommendation for the Transitioning of Cryptographic Algorithms and Key Lengths” (http://csrc.nist.gov/publications/drafts/800-131/draft-sp800-131_spd-june2010.pdf). At the time of writing the second round of public comments had just finished, so note that transitioning may not go ahead according to the schedule described in this draft.

*56 New European Schemes for Signatures, Integrity and Encryption. A cryptographic algorithm evaluation project carried out by the EU (<http://cordis.europa.eu/ist/>) fund between 2000 and 2003.

*57 NESSIE, “Portfolio of recommended cryptographic primitives” (<https://www.cosic.esat.kuleuven.be/nessie/deliverables/decision-final.pdf>).

*58 Bekanntmachung zur elektronischen Signatur nach dem Signaturgesetz und der Signaturverordnung (Übersicht über geeignete Algorithmen) (<http://www.bundesnetzagentur.de/cae/servlet/contentblob/148572/publicationFile/3994/2010AlgoKatpdf.pdf>) (in German).

*59 Mécanismes cryptographiques. Règles et recommandations concernant le choix et le dimensionnement des mécanismes cryptographiques (http://www.ssi.gouv.fr/IMG/pdf/RGS_B_1.pdf) (in French).

In Japan, CRYPTREC^{*60} announced the e-Government Recommended Ciphers List^{*61} in February 2003. The information accompanying this list recommends algorithms with 128 bits of security for symmetric key cryptography and hash functions. Recommended key lengths for public key cryptography were described in two guidebooks^{*62*63}, but there was no information regarding the transition schedule.

In Japan the National Information Security Center (NISC) is currently coordinating ministries with regard to the cryptographic algorithms used for government agency information systems. The guidelines regarding the transition of SHA-1 (while not actively recommended, it appears on the 2002 e-Government Recommended Ciphers List) and RSA-1024^{*64} were approved at the 17th assembly of the Information Security Policy Council (April 22, 2008), and details of the progress made towards this were disclosed at the 20th assembly (February 3, 2009)^{*65}. Regarding the cryptographic algorithms used for government agency information systems, it is expected that use of SHA-256 and RSA-2048 will begin in 2014, and use of SHA-1 and RSA-1024 will be discontinued in 2017 after a grace period of three years. The three year grace period depends on the expiration dates of public key certificates, so some believe it may be extended to five years.

The U.S. and France are carrying out the transition over two stages (a medium-term plan transitioning to 100 bits and 112 bits of security, and a long-term plan transitioning to 128 bits of security). However, the plan currently being drafted in Japan only covers the scope of the first of these stages, and it is believed that a plan for securing a higher level of security such as a transition to 128 bits of security will be drawn up in the future.

Figure 9 shows the state of previous compromises of major cryptographic algorithm standards and developments in each of the countries mentioned above.

■ Year 2010 Issues on Cryptographic Algorithms: Impact and Countermeasures

It was initially thought that the Year 2010 Issues on Cryptographic Algorithms that originate from NIST's policy would result in a full transition by the end of 2010. However, as currently indicated by NIST's SP800-131 draft, it is becoming clear that there will be no unexpected transition problems by the end of 2010. Meanwhile, early transition is being prepared with a focus on certification authorities whose business is founded on public key infrastructure (PKI), with

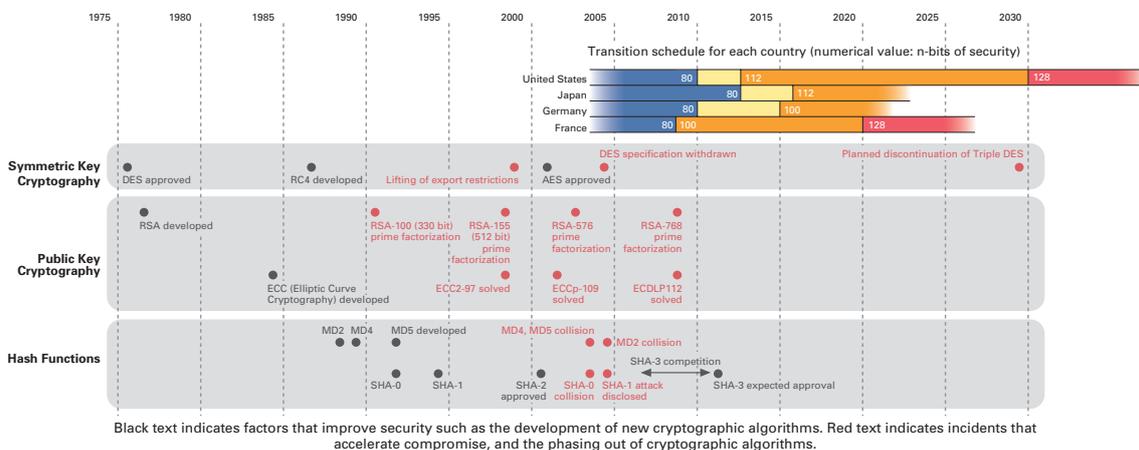


Figure 9: Cryptographic Algorithm Transition Schedule

*60 CRYPTREC: Cryptography Research and Evaluation Committees (<http://www.cryptrec.go.jp/english/>). This is a project for evaluating and monitoring the security of e-government recommended ciphers and examining the establishment of cryptographic module validation standards. It is jointly managed by the Ministry of Internal Affairs and Communications and the Ministry of Economy, Trade and Industry.

*61 e-Government Recommended Ciphers List (<http://www.cryptrec.go.jp/english/list.html>).

*62 CRYPTREC, "Guidebook for e-Government recommended ciphers" (http://www.cryptrec.go.jp/report/c07_guide_final_v3.pdf) (in Japanese).

*63 CRYPTREC, "List guide 2008 (Digital signature)" (http://www.cryptrec.go.jp/report/c08_listguide2008_signature_v7.pdf) (in Japanese).

*64 Transition Guidelines concerning the Cryptographic Algorithms SHA-1 and RSA1024 Adopted by Government Agencies (http://www.nisc.go.jp/active/general/pdf/crypto_pl.pdf) (in Japanese).

*65 Details of the progress made based on the "Transition Guidelines concerning the Cryptographic Algorithms SHA-1 and RSA1024 Adopted by Government Agencies" (<http://www.nisc.go.jp/conference/seisaku/dai20/pdf/20siryou0502.pdf>) (in Japanese).

various PKI vendors announcing that they will deal with Year 2010 Issues since the beginning of this year^{*66*}^{*67}. For EV certificates^{*68} in particular the CA/Browser Forum^{*69} has established issuing guidelines that take compromise into consideration, and public key certificates with an expiration date falling in 2011 or later can no longer use RSA-1024, instead being restricted to RSA-2048. Additionally, algorithms using SHA-256 or greater are recommended for hash functions, and the use of SHA-1 is only permitted until the SHA-2 family is included in the majority of Web browsers (an exact time frame has not been specified).

The impact of the Year 2010 Issues on Cryptographic Algorithms is more widespread than PKI and public key certificates. NIST has provided detailed recommended configuration values for protocols such as SSL/TLS, S/MIME, and DNSSEC^{*70}. Transitions to SHA-2 and RSA-2048 are also under review for time business such as time stamps and archiving signatures^{*71}.

Let us consider how to address the Year 2010 Issues on Cryptographic Algorithms. As individual cryptographic algorithms are not compatible, transition requires that the algorithms themselves be replaced. This transition can be separated into two phases. The first phase involves including new cryptographic algorithms in Web browsers and other software through updates. However, as demonstrated by efforts to end the use of Internet Explorer version 6^{*72}, it is generally difficult to force end users to update. It has also been noted that transition is even more difficult for mobile phones and game devices than for PCs^{*73}.

The second phase involves phasing out compromised algorithms. As can be seen from the NIST's approach of using a "Deprecated" status, when users use cryptographic algorithms with low security it is necessary to make them aware of the risk involved. As an example of this risk, there have been cases reported in which connections have been made using compromised algorithms due to the user settings of older Web browser versions^{*74}. Additionally, as some devices such as mobile phones do not support RSA-2048, it is possible that administrators may hesitate to exclude certificates with low security on the server side due to apprehension regarding costs and loss of opportunity.

■ Summary

As shown here, cryptographic algorithms are compromised as time passes, and the level of security they provide deteriorates. This is not unique to the Year 2010 Issues we have introduced here, as it has also occurred in the past (for example with 56 bit DES), and it will continue to occur in the future. Consequently, when using cryptographic algorithms and their implementations, it is necessary to ensure that they offer sufficient security for the period they are used.

In Japan, CRYPTREC is currently considering revising the e-Government Recommended Ciphers List^{*75}. This will involve revision of the current 2002 version of the list^{*76}, and it will affect government procurement. It will be

*66 VeriSign 2048 bit Root Migration, (<https://knowledge.verisign.com/support/ssl-certificates-support/index?page=content&id=AD220>).

*67 Entrust Certificate Services Support Knowledge Base, TN 7710 - Entrust is moving to 2048-bit RSA keys. Why? (<http://www.entrust.net/knowledge-base/technote.cfm?tn=7710>).

*68 Extended Validation SSL Certificate. Intended to indicate sites with improved security to users, as the URL input field will turn green when viewing an SSL/TLS site on a browser, and they undergo more rigorous vetting in comparison to the issuing criteria for previous SSL server certificates.

*69 CA/Browser Forum (<http://www.cabforum.org/>), "Guidelines For The Issuance And Management Of Extended Validation Certificates" (http://www.cabforum.org/Guidelines_v1_2.pdf). Appendix A "Minimum Cryptographic Algorithm and Key Sizes" contains information on recommended algorithms and key lengths for 2010 and beyond.

*70 NIST Special Publication 800-57 Recommendation for Key Management - Part 3: Application-Specific Key Management Guidance (http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57_PART3_key-management_Dec2009.pdf).

*71 Time-Stamping Service Accreditation Center, "Commencement of review into the transition of cryptographic algorithms for TSA and TA services using digital signatures" (<http://www.dekyo.or.jp/tb/data/100708.pdf>) (in Japanese).

*72 National Information Security Center, "Regarding efforts to transition from older browsers to newer browsers" (http://www.nisc.go.jp/press/pdf/browser_transition_press.pdf) (in Japanese).

*73 Matsumoto and Une, "The Current State of and Future Prospects for SSL Certificate Cryptographic Algorithm Transition", Institute for Monetary and Economic Studies, Bank of Japan, Discussion Paper No. 2010-J-11 (<http://www.imes.boj.or.jp/japanese/jdps/2010/10-J-11.pdf>) (in Japanese).

*74 Kanda, "The Current State of and Issues regarding TLS/SSL Cryptography Use", Internet Week 2009 (<http://www.nic.ad.jp/ja/materials/iw/2009/proceedings/h9/iw2009-h9-04.pdf>) (in Japanese).

*75 Start of the Application for Cryptographic Techniques towards the Revision of the e-Government Recommended Ciphers List (http://www.cryptrec.go.jp/english/topics/cryptrec_20091001_application_open.html).

*76 Policy for the use of ciphers to be used for information system procurement of each agency, February 28, 2003 (http://cryptrec.go.jp/images/cryptrec_02.pdf) (in Japanese).

necessary to keep track of future trends, such as whether the upcoming 2013 version of the list will include key length restrictions, or whether it will be consistent with the next NISC transition guidelines to be announced.

1.4.2 Observations on Backscatter Caused by DDoS Attacks

Sometimes hosts connected to the Internet receive unwanted packets that should not have been sent to them. Of these packets, those that attempt to initiate communications are considered to have been sent by malware or attack tools to locate suitable targets to attack, and we have examined the status of these random communications in this report under “1.3.2 Malware Activities” in the past. However, among the unwanted packets observed, we also frequently see packets other than those that attempt to initiate communications that would be classified as responses under protocol specifications arriving in an unexpected fashion. These response packets that arrive out of the blue may be “backscatter packets” that occur as a side effect of DDoS attacks on a host situated somewhere on the Internet. Here, we examine the mechanism by which backscatter packets occur, and how this can be applied to the observation of DDoS attacks.

■ How Backscatter Occurs

As already mentioned in “1.3.1 DDoS Attacks,” DDoS attacks generally involve sending a large volume of packets to the target host. The host that is targeted by the attack sends back packets in response to the packets received based on TCP/IP specifications (Table 3). If the original attack packets misrepresent the sender’s IP address randomly (IP spoofing), these response packets are returned to the spoofed IP addresses rather than the original sender. This is the phenomenon called backscatter that occurs as a side effect of DDoS attacks. Figure 10 shows a depiction of the occurrence of backscatter packets.

A technique called “backscatter analysis” indirectly estimates DDoS attacks on the Internet using this backscatter phenomenon^{*77}. An observing host connects to the Internet, and when it obtains incoming backscatter packets, the sender’s IP address indicates the IP address of a server thought to be experiencing a DDoS attack. A large number of reports using this technique have been published to date^{*78}. Attempts to estimate the magnitude of attack traffic (the number of packets per unit of time, etc.) using the frequency of incoming backscatter packets are also being made by carrying out probabilistic calculation based on a number of hypotheses.

Table 3: Major Incoming Packets and Responses Determined by the TCP/IP Specifications

Incoming Packet	Response Packet
TCP SYN	TCP SYN/ACK (If the port is in service)
TCP SYN	TCP RST (If the port is not in service)
TCP DATA	TCP RST
TCP RST	No response
ICMP Echo Request	ICMP Echo Reply
UDP	Depends on the upper layer protocol (If the port is in service)
UDP	ICMP Port Unreachable (If the port is not in service)

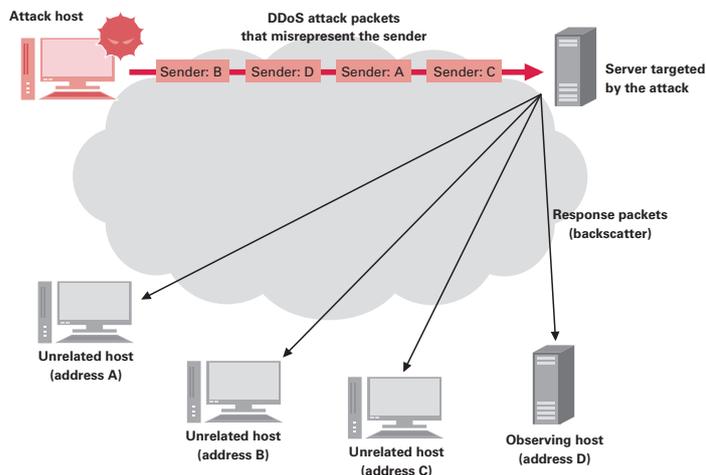


Figure 10: The Occurrence of DDoS Backscatter

*77 The following research was presented at the USENIX Security Symposium held in 2001. David Moore, Geoffrey M. Voelker, Stefan Savage, “Inferring Internet Denial-of-Service Activity” (<http://www.usenix.org/events/sec01/moore.html>).

*78 For example, the following annual report on information technology analysis published by the National Police Agency of Japan contains a report employing backscatter analysis. “Information Technology Analysis Annual Report 2009” (http://www.npa.go.jp/cyberpolice/detect/pdf/H21_nempo.pdf) (in Japanese), and separate volume (http://www.npa.go.jp/cyberpolice/detect/pdf/H21_betsu.pdf) (in Japanese).

■ MITF Backscatter Observations

Packets thought to be backscatter have also been observed in the honeypots managed by the MITF that IIJ operates. Here, we present the results of our observations for July 2010.

Figure 11 shows trends in the sender's addresses by country for backscatter packets observed during this month, and Figure 12 shows the distribution by country for the entire period. Figure 13 shows sender port trends, and Figure 14 shows distribution by port for the entire period. An average of 4,611 packets were detected per day for the entire period under study.

Classified by country the majority of backscatter was accounted for by China at 51.8% and the United States at 24.9%, indicating that hosts in these countries experienced a large number of attacks that spoofed IIJ IP addresses. However, it is possible that attack packet IP address spoofing is not completely random, so it should be noted that it is not possible to compare attack volume size using this data alone. Classified by port the 80/TCP port used for Web services was observed most often, accounting for 57.6% of the total. Other than 80/TCP, well-known ports such as 21/TCP used for FTP came up occasionally, but ports such as those used by online games and ports of an unspecified use were also detected. The majority of backscatter packets from these ports originated in China.

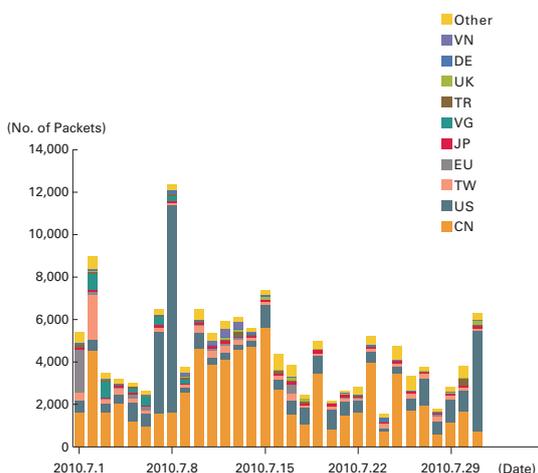


Figure 11: Backscatter Packet Trends by Sender's Country

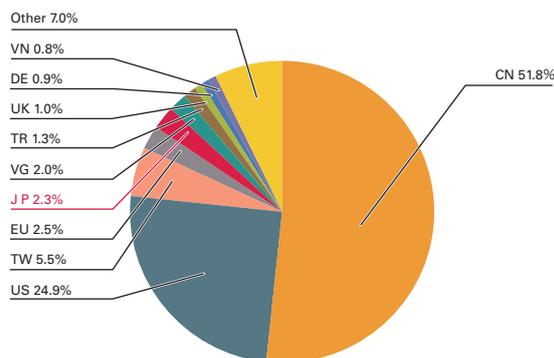


Figure 12: Distribution by Country for the Entire Period under Study

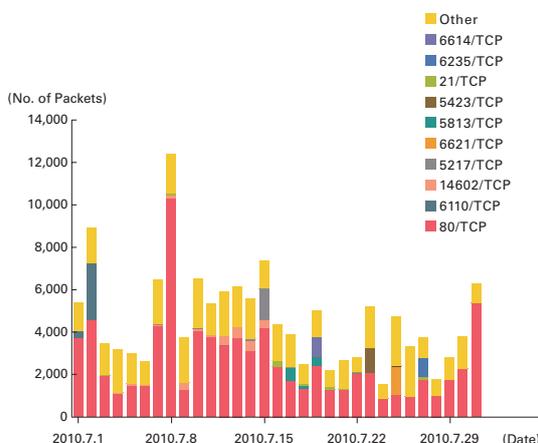


Figure 13: Backscatter Packet Trends by Sender's Port

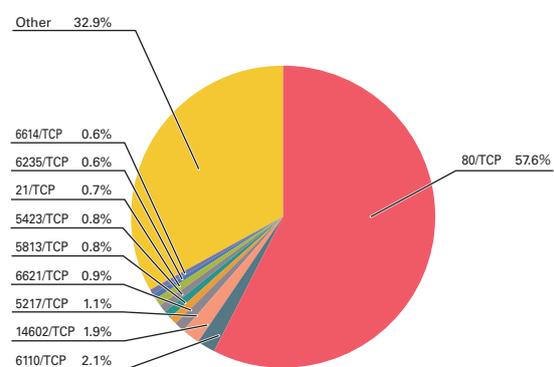


Figure 14: Distribution by Port for the Entire Period under Study

Next, we extracted the backscatter packets sent from the Web services 80/TCP port, and show our analysis of the most common sender's addresses in the figure below (Figure 15). As an example of a particularly large volume of observed backscatter packets, we observed a total of 12,901 packets from the IP address of a Web hosting company in the United States between July 7 and 8. A number of websites are hosted at this IP address, but it was confirmed that all were sites distributing Chinese content. In other words, although the IP address was based in the United States, we believe that Chinese companies were targeted in the attacks. Between July 10 and 16, a total of 13,408 packets were observed from an IP address in China.

In addition to these, backscatter packets were observed from the IP address for a Canadian company on July 1, from a Taiwan IP address on July 2, and from a British Virgin Islands IP address between July 2 and 6. Between July 16 and 23 backscatter packets were observed from an IP address belonging to a Web hosting company in the United States unrelated to the one mentioned previously. Multiple company websites are hosted at this address, and most of them were sites containing Turkish content.

As shown here, it was observed that for Web services company websites from a variety of countries were the main targets of attacks.

■ Backscatter Observation Limits and Applications

As shown above, backscatter analysis can be applied to the observation of DDoS attacks. However, only a portion of DDoS attack types can be detected using this technique (Figure 16). For example, backscatter does not occur in attacks that do not or cannot easily misrepresent IP addresses, such as HTTP GET flood attacks. Backscatter is also not generated in attacks using packets that do not require a response such as TCP RST. Servers targeted in an attack may also return almost no response packets due to the overload or their settings.

Even when backscatter packets are observed, it is not possible to obtain detailed information required to respond to an attack. For example, because backscatter occurs as a result of spoofed IP addresses, it is not possible to identify the original attack source. Furthermore, in all but very few cases, it is also not possible to estimate the attack volume (total bandwidth, etc.).

Indirect observation of DDoS attacks using backscatter is limited in this way, and is not a substitute for direct observation. However, it does have the benefit of allowing DDoS attacks occurring on external networks to be detected and observed by third parties without intervening, and it can serve as a complement to direct observation. We believe that by gathering a large quantity of information on DDoS attacks in this way we can contribute to the detection of and countermeasures for DDoS attacks that occur in Japan.

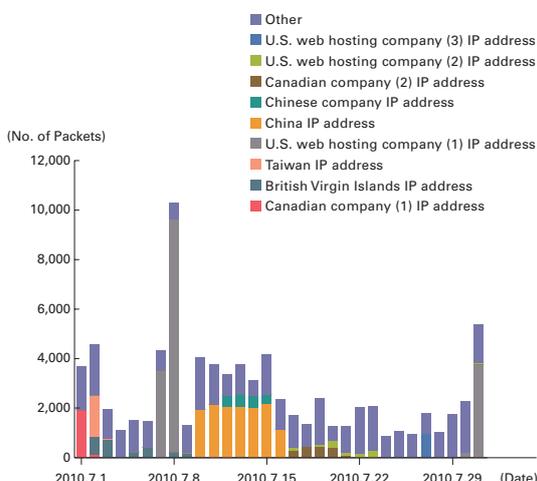


Figure 15: Backscatter Packets from Port 80/TCP

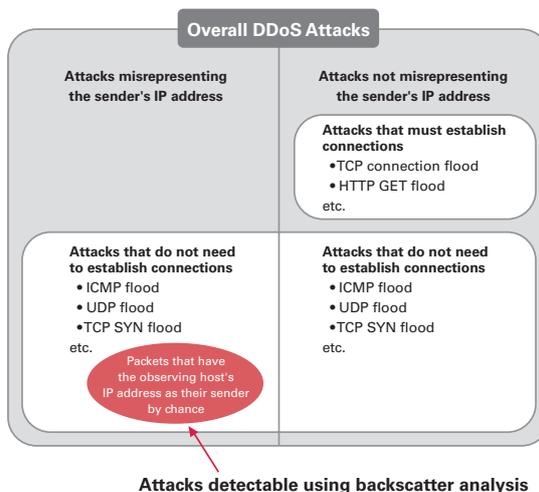


Figure 16: DDoS Attacks Detectable Using Backscatter Analysis

1.4.3 Trends in Vulnerability Information Circulation

Vulnerabilities exist in some form or other for all software and hardware that connects to the Internet. Vulnerabilities that would be security threats if exploited include not only implementation issues such as programming bugs, but also issues that arise through external factors such as processing capacity limitations that occur due to changes in Internet usage. For those who manage systems, identifying vulnerabilities and dealing with them appropriately at an early stage is a crucial part of maintaining system security. However, while it is necessary to disseminate information regarding vulnerabilities^{*79}, this information itself can also be exploited, so sufficient care must be taken when handling it. Here, we describe the process adopted in Japan of discovering a vulnerability, notifying vendors, creating countermeasures, and disclosing information in a quick and efficient manner, and also introduce criteria for users to evaluate the importance of vulnerability information.

■ JVN and the Information Security Early Warning Partnership

Examples of reference material for vulnerability countermeasures include the Vulnerability Notes Database (US-CERT VN)^{*80}, which endeavors to aggregate and disclose information regarding vulnerabilities, and Common Vulnerabilities and Exposures (CVE)^{*81}, which can be used like a dictionary to reference vulnerabilities using their unique identifiers. However, the fact that this information is all in English (thus hard to read for most Japanese readers) and contains little information on products in Japan has been a problem in the past.

To aggregate information about vulnerabilities and their fixes for products used in Japan, such as Japanese word processors and personal routers, and make this available for more users in Japan to reference, there is a need to supply information in Japanese. For this reason, the JPCERT/CC Japanese Vulnerability Notes (JVN) project^{*82} was established in February 2003.

Taking into account deliberations at an IPA study group in April 2004^{*83}, and based on Ministry of Economy, Trade and Industry (METI) Notice No.235^{*84}, the Information Security Early Warning Partnership^{*85} was established in July 2004 as a system for circulating vulnerability information among product developers.

Under this partnership, through METI Notice No.236, IPA is designated as the authority for receiving vulnerability information, and JPCERT/CC as the authority for coordinating with product developers. These two organizations collaborate to communicate with product developers and reporters of vulnerability information, coordinate release dates between product developers, and handle the process through to the eventual collection and release of information about countermeasures for each product. As part of this partnership JVN currently serves as a repository for information released by product developers, and it is jointly operated by JPCERT/CC and IPA. In April 2007 JVN iPedia^{*86} was also released, containing information from other sources, vulnerability threat evaluation, and countermeasures in addition to the vulnerability information handled under this partnership.

These activities not only facilitated the circulation of vulnerability information about products in Japan, but have also been highly commended internationally due to them being a progressive approach of vulnerability countermeasures

*79 Examples of public forums for sharing and discussing vulnerability information include BugTraq (<http://www.securityfocus.com/archive/1>) and Full-Disclosure (<http://lists.grok.org.uk/full-disclosure-charter.html>).

*80 The CERT/CC Vulnerability Notes Database. It subsequently became the US-CERT Vulnerability Notes Database (<http://www.kb.cert.org/vuls/>). IJ also provides information regarding its SEIL router products (<http://www.seil.jp/>).

*81 Common Vulnerabilities and Exposures, CVE (<http://cve.mitre.org/>). A unique CVE-ID is assigned to each specific vulnerability to make clear distinction among similar but different vulnerabilities. CVE is operated by the U.S. MITRE Corporation, but there are multiple CNA (CVE Numbering Authority) organizations for assigning CVE-IDs, and in Japan JPCERT/CC was authorized as a CNA in June 2010 (http://www.jpCERT.or.jp/press/2010/PR20100624_cna.pdf) (in Japanese).

*82 Japan Vulnerability Notes (<http://jvn.jp/en/>). Initially released as a JPCERT/CC project, it is currently jointly operated by JPCERT/CC and IPA.

*83 IPA "Study Group for the Handling of Vulnerability Information for Information Systems, etc." report (<http://www.ipa.go.jp/about/press/20040406.html>) (in Japanese).

*84 Standards for Handling Software Vulnerability Information (2004 Ministry of Economy, Trade and Industry Notice No.235) (http://www.meti.go.jp/policy/netsecurity/law_guidelines.htm) (in Japanese).

*85 Ministry of Economy, Trade and Industry, Regarding the Start of the "Information Security Early Warning Partnership" (http://www.meti.go.jp/policy/it_policy/press/0005399/) (<http://www.ipa.go.jp/security/vuln/report/>) (<http://www.jpCERT.or.jp/vh/>) (in Japanese). IJ has participated in this partnership as a product developer since the start of operations.

*86 JVN iPedia (<http://jvndb.jvn.jp/en/>)

in which national and public agencies have played a leading role, and due to the fact that information unique to Japan is translated into English and details of the situation in Japan disseminated around the world.

Other vulnerability information available for use today includes the U.S. government's NSD standard vulnerability database^{*87} operated by the National Institute of Standards and Technology (NIST), the OSVDB^{*88} maintained by a nonprofit organization, the Open Security Foundation, and databases operated by IT security companies^{*89}.

■ Evaluation of Vulnerability Information

Software and product vendors are currently making efforts to distribute vulnerability patches and firmware updates automatically. However, patches and firmware updates such as these may include new functions in addition to vulnerability fixes, and even when applied specifically to fix a vulnerability, changes are sometimes made to existing functions including the settings interface. Additionally, when using applications of their own or with unique customization such as those seen at many Japanese companies, time is also required for carrying out compatibility tests. Furthermore, if rebooting is required after a patch is applied, the timing of patches must be coordinated for systems that demand continuous operation.

Consequently, from the perspective of those receiving vulnerability information it is also necessary to consider the details of vulnerability information, and determine whether or not to apply a vulnerability patch and the best time to do it. For this reason, there is a need to evaluate the threat that a vulnerability poses, taking factors such as the ease that it can be exploited, the severity of its repercussions, and its impact on systems into consideration. CVSS (Common Vulnerability Scoring System)^{*90} can be used as a measurement index for providing information from vendors about the threat of vulnerabilities and aiding users in making decisions appropriate for their environment. CVSS vulnerability threat evaluation standards are composed of base metrics, temporal metrics, and environmental metrics.

The base metrics evaluate how easy a vulnerability is to exploit, and the impact on security CIA (Confidentiality, Integrity, and Availability) when a vulnerability is exploited. The temporal metrics indicate how easy a vulnerability is to exploit at the current point in time, such as whether attack code exists, whether a patch is available, and the credibility of vulnerability information. Finally, environmental metrics evaluate whether there is potential for collateral damages when a vulnerability is attacked in a certain environment, as well as how many systems have a particular vulnerability, and the degree of security required for the CIA of a given system.

In many cases the base metrics and temporal metrics are provided by product and security vendors, but environment metrics include items for users to set according to their environment. Threat is evaluated using a certain formula after first evaluating each item^{*91}. This evaluation can be recalculated any number of times in response to changing circumstances, such as the release of a patch or the appearance of code exploiting a vulnerability, making it possible for users to correctly evaluate the current level of threat.

Standards other than CVSS that allow users to reference threat evaluation include JPCERT/CC's independent evaluation of information available on JVN^{*92}. The Microsoft Exploitability Index^{*93} is also worth referencing, as it adds information

*87 National Vulnerability Database (<http://nvd.nist.gov/>).

*88 The Open Source Vulnerability Database (<http://osvdb.org/>).

*89 For example the IBM ISS Threat List (<http://www.iss.net/threats/ThreatList.php>) or Denmark's Secunia (<http://secunia.com/>). There is also France's VUPEN Security service (<http://www.vupen.com/english/>), which provides undisclosed vulnerability information to its customers.

*90 CVSS is designed and operated by FIRST's CVSS-SIG (<http://www.first.org/cvss/>). See the following materials for information regarding the values set for each evaluation item in the CVSS 2.0 standard currently in use. "A Complete Guide to the Common Vulnerability Scoring System Version 2.0" (<http://www.first.org/cvss/cvss-guide.html>). For information in Japanese, see the following IPA article. "The CVSS Common Vulnerability Scoring System" (<http://www.ipa.go.jp/security/vuln/CVSS.html>). However, this article also gives the settings for each item in Japanese, so it is advisable to use the FIRST guide alongside this when actually carrying out an evaluation using settings information given in English.

*91 IPA's CVSS calculator (<http://jvndb.jvn.jp/cvss/en.html>) is an example of a system that automates CVSS calculation.

*92 JPCERT/CC applies its own scoring system divided into the categories "Access required," "Authentication," "User interaction required," and "Exploit complexity" according to the exploitation status of a vulnerability (<http://jvn.jp/en/nav/jvnhelp.html>).

*93 The Microsoft Exploitability Index provides a three level assessment (Consistent exploit code likely, Inconsistent exploit code likely, Functioning exploit code unlikely) of exploitation of a given vulnerability based on whether or not proof-of-concept code or exploit code exists as well as actual instances of exploitation. See the following description for details regarding the Exploitability Index (<http://technet.microsoft.com/en-us/security/cc998259.aspx>).

such as exploitation incidents and their prevalence. Additionally, information that includes patch details and the usage of an affected system such as the ISC ratings*⁹⁴ assigned by SANS ISC has become increasingly available.

■ Summary

In this section we have introduced activities in Japan that facilitate the smooth circulation of vulnerability information, and useful standards for users to evaluate this information.

Regarding the handling of vulnerability information, there have been moves to compensate reporters of vulnerability information*⁹⁵ and introduce SCAP*⁹⁶ for promoting the circulation of vulnerability countermeasure information and automating said countermeasures, and from a user's perspective these things may greatly effect the handling of vulnerability information in years to come. We would like to examine these related activities at some point in the future.

1.5 Conclusion

This report has provided a summary of security incidents to which IJ has responded. In this report, rather than dealing with specific incidents, we have summarized various countries' stances on the Year 2010 Issues on Cryptographic Algorithms, analyzed backscatter as a method of observing DDoS attacks, and examined trends in the vulnerability information circulation.

By identifying and publicizing incidents and associated responses in reports such as this, IJ will continue to inform the public about the dangers of Internet usage, providing the necessary countermeasures to allow the safe and secure use of the Internet.

Authors:

Mamoru Saito

Manager of the Office of Emergency Response and Clearinghouse for Security Information, IJ Service Division. After working in security services development for enterprise customers, Mr. Saito became the representative of the IJ Group emergency response team, IJ-SECT in 2001, participating in FIRST, an international group of CSIRTs. Mr. Saito serves as a steering committee member of several industry groups, including Telecom-ISAC Japan, Nippon CSIRT Association, Information Security Operation provider Group Japan, the Web Malware Mitigate Community, and others. In recognition of its close activities with both domestic and international organizations, the IJ-SECT was awarded the "commendation from Director-General, Commerce and Information Policy Bureau, Ministry of Economy, Trade and Industry (CATEGORY - Promotion of Information Security)" at the FY 2009 Informatization Month Opening Ceremony.

Hirohide Tsuchiya (1.2 Incident Summary)

Hirohide Tsuchiya, Hiroshi Suzuki (1.3 Incident Survey)

Yuji Suga (1.4.1 Trends in the Year 2010 Issues on Cryptographic Algorithms)

Tadaaki Nagao (1.4.2 Observations on Backscatter Caused by DDoS Attacks)

Mamoru Saito (1.4.3 Trends in Vulnerability Information Circulation)

Office of Emergency Response and Clearinghouse for Security Information, IJ Service Division

Contributors:

Masahiko Kato, Hiroaki Yoshikawa, Hiroshi Suzuki

Office of Emergency Response and Clearinghouse for Security Information, IJ Service Division

*94 ISC ratings list the fixes included in specific Microsoft patches, the corresponding KB, whether or not there are known exploits, and the exploitability index, while also evaluating the possibility of attack for both client and server systems and rating the urgency as Less Urgent, Important, Critical, or PATCH NOW. For examples, see (<http://isc.sans.edu/diary.html?storyid=8929>) for scheduled patches in June 2010, and (<http://isc.sans.edu/diary.html?storyid=9166>) for scheduled patches in July 2010.

*95 Google's open-source project "The Chromium Project" pays \$500 to providers of vulnerability information (<http://blog.chromium.org/2010/01/encouraging-more-chromium-security.html>). The Zero Day Initiative hosted by HP TippingPoint also rewards those who provide vulnerability information (<http://www.zerodayinitiative.com/about/benefits/>).

*96 Security Content Automation Protocol. This is an information-sharing format and protocol suite for standardizing and automating security measures for organizations related to the U.S. government that is prescribed by the National Institute of Standards and Technology. CVE and CVSS that are introduced in this report are constituent elements of this protocol. The JVN iPedia provided by IPA also uses elements of SCAP, and is a leading-edge implementation of SCAP in Japan.