International Standards for Cloud Security

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 October 1 through December 31, 2015. In this period a number of hacktivism-based attacks were once again carried out by Anonymous and other groups, and there were frequent incidents that included many DDoS attacks, information leaks caused by unauthorized access, and website defacements. Operations mainly aimed at Japan were also carried out, and a number of websites including those for government institutions were targeted in DDoS attacks. There were a large number of DDoS attacks accompanied by threats such as demands for financial compensation via virtual currency, and it can be confirmed that multiple groups are active. There were also many information leaks caused by unauthorized access, such as the leak of a large amount of personal information including credit card details centered around U.S. hotel chains. These examples show that many security-related incidents continue to occur on the Internet.

1.2 Incident Summary

Here, we discuss the IIJ handling and response to incidents that occurred between October 1 and December 31, 2015. Figure 1 shows the distribution of incidents handled during this period*1.

■ The Activities of Anonymous and Other Hacktivists

Attacks by hacktivists such as Anonymous continued during this period. DDoS attacks and information leaks occurred at government-related and corporate sites in a large number of countries stemming from a variety of incidents and causes.

During this survey period, individuals and organizations thought to be associated with ISIL or sympathetic to its principles continued to carry out website defacements and SNS account hijackings around the world. In revenge for the coordinated terrorist attacks in Paris, Anonymous identified and froze SNS accounts related to ISIL (OpParis). In December there were large-scale DDoS attacks on DNS servers for Turkey's .tr domains based on claims that the Turkish government supports ISIL. These attacks took place over several days, and also affected RIPE, which serves as a secondary DNS for Turkish domains*2. In addition to attacks on DNS servers, there were also attacks targeting Turkish government institutions and major banks. DDoS attacks targeting the website of U.K. broadcaster the BBC also took place, with an anti-ISIL group claiming responsibility.

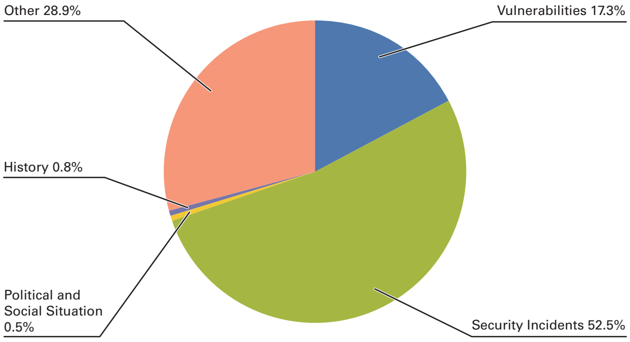


Figure 1: Incident Ratio by Category (October 1 to December 31, 2015)

In the Middle East, the website of an Israeli radio station was defaced in October, and the Twitter account of an Israeli newspaper publisher was hijacked and used to post messages in November. The website of the Israeli Missile Defense Association was also accessed without authorization, leading to the leak of user data. As this demonstrates, attacks on Israeli government-related sites and the websites of private sector corporations continue to occur.

[1] Incidents discussed in this report are categorized as vulnerabilities, political and social situations, history, security incidents or other.
Vulnerabilities: Responses to vulnerabilities associated with network equipment, server equipment or software commonly used over the Internet or 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: Unexpected incidents and related responses such as wide propagation of network worms and other malware; DDoS attacks against certain websites.
Other: Security-related information, and incidents not directly associated with security problems, including highly concentrated traffic associated with a notable event.

[2] See the following email archive for the RIPE DNS-WG for more information about the attacks. "[dns-wg] RIPE NCC Authoritative and Secondary DNS services on Monday 14 December" (https://www.ripe.net/ripe/mail/archives/dns-wg/2015-December/003184.html).

Since September, DDoS attacks thought to have been perpetrated by Anonymous as part of protests against the drive fishing of dolphins and small whales have temporarily rendered the website of Taiji-cho in Wakayama Prefecture inaccessible (OpKillingBay, OpWhales). Attacks based on these operations have targeted not only Japan, but also organizations such as the World Association of Zoos and Aquariums (WAZA) and the Convention on International Trade in Endangered Species of Wild Fauna and Flora (CITES). In Japan, attacks on the websites of related organizations and local authorities, as well as airport companies and the personal website of the prime minister, were still being carried out repeatedly in October. The attack methods have been changing, with information leaks thought to be caused by SQL injection attacks also carried out in addition to DDoS attacks. Furthermore, it has been identified that organizations not directly related to the protest activities, such as news outlets, ISPs, and publishers, have also begun to be targeted by attacks. As of January at the time of writing, attacks on a number of organizations including Japanese government institutions were still ongoing, so continued vigilance is necessary.

In the United States, attacks were made on websites linked to candidates that have demonstrated extreme views and behavior in relation to the presidential primaries. A list of the SNS pages of people thought to be supporters of a U.S. secret society was also released. Other attacks by hacktivists such as Anonymous continue on government and government-related websites around the world.

Vulnerabilities and their Handling

During this period, fixes were released for Windows[*3][*4][*5][*6][*7], Internet Explorer[*8][*9][*10], Office[*11][*12][*13], and Edge[*14]. Updates were also made to Adobe Systems' Flash Player, Acrobat, and Reader. A quarterly update was released for Oracle's Java SE, fixing many vulnerabilities. Several of these vulnerabilities were exploited in the wild before patches were released.

Regarding server applications, a quarterly update was released for a number of Oracle products, including the Oracle database server, fixing many vulnerabilities. Multiple vulnerabilities were also discovered and fixed in ntpd, including those that could bypass authentication and allow manipulation of system time settings, and those that could be exploited to carry out DoS attacks using specially-crafted packets. A vulnerability in BIND9 DNS servers that could allow DoS attacks via requests for records with a malformed class attribute was discovered and fixed. Vulnerabilities including those that could be exploited in open redirect attacks were also discovered and fixed in the Drupal CMS[*15]. A number of vulnerabilities, including those that could allow remote code execution by a third party, were discovered and fixed in the Joomla! CMS. Several vulnerabilities that could allow arbitrary

[*3] "Microsoft Security Bulletin MS15-109 - Critical: Security Update for Windows Shell to Address Remote Code Execution (3096443)" (https://technet.microsoft.com/en-us/library/security/ms15-109.aspx).

[*4] "Microsoft Security Bulletin MS15-111 - Important: Security Update for Windows Kernel to Address Elevation of Privilege (3096447)" (https://technet.microsoft.com/en-us/library/security/ms15-111.aspx).

[*5] "Microsoft Security Bulletin MS15-126 - Critical: Cumulative Security Update for JScript and VBScript to Address Remote Code Execution (3116178)" (https://technet.microsoft.com/en-us/library/security/ms15-126.aspx).

[*6] "Microsoft Security Bulletin MS15-128 - Critical: Security Update for Microsoft Graphics Component to Address Remote Code Execution (3104503)" (https://technet.microsoft.com/en-us/library/security/ms15-128.aspx).

[*7] "Microsoft Security Bulletin MS15-135 - Important: Security Update for Windows Kernel-Mode Drivers to Address Elevation of Privilege (3119075)" (https://technet.microsoft.com/en-us/library/security/ms15-135.aspx).

[*8] "Microsoft Security Bulletin MS15-106 - Critical: Cumulative Security Update for Internet Explorer (3096441)" (https://technet.microsoft.com/en-us/library/security/ms15-106.aspx).

[*9] "Microsoft Security Bulletin MS15-112 - Critical: Cumulative Security Update for Internet Explorer (3104517)" (https://technet.microsoft.com/en-us/library/security/ms15-112.aspx).

[*10] "Microsoft Security Bulletin MS15-124 - Critical: Cumulative Security Update for Internet Explorer (3116180)" (https://technet.microsoft.com/en-us/library/security/ms15-124.aspx).

[*11] "Microsoft Security Bulletin MS15-110 - Important: Security Updates for Microsoft Office to Address Remote Code Execution (3096440)" (https://technet.microsoft.com/en-us/library/security/ms15-110.aspx).

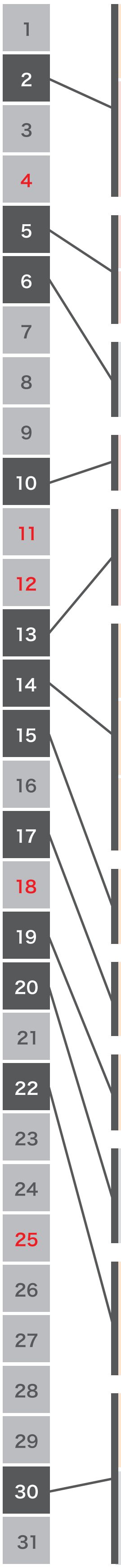
[*12] "Microsoft Security Bulletin MS15-116 - Important: Security Update for Microsoft Office to Address Remote Code Execution (3104540)" (https://technet.microsoft.com/en-us/library/security/ms15-116.aspx).

[*13] "Microsoft Security Bulletin MS15-131 - Critical: Security Update for Microsoft Office to Address Remote Code Execution (3116111)" (https://technet.microsoft.com/en-us/library/security/ms15-131.aspx).

[*14] "Microsoft Security Bulletin MS15-125 - Critical: Cumulative Security Update for Microsoft Edge (3116184)" (https://technet.microsoft.com/en-us/library/security/ms15-125.aspx).

[*15] "Drupal Core - Overlay - Less Critical - Open Redirect - SA-CORE-2015-004" (https://www.drupal.org/SA-CORE-2015-004).

October Incidents



V **2nd: A vulnerability (CVE-2015-6602) in Android's libutils that could allow arbitrary code execution via specially-crafted files was discovered and fixed.** See the following Zimperium, Inc. blog post for more details. "Zimperium zLabs is Raising the Volume: New Vulnerability Processing MP3/MP4 Media." (https://blog.zimperium.com/zimperium-zlabs-is-raising-the-volume-new-vulnerability-processing-mp3mp4-media/).

S **2nd: Experian Information Solutions, Inc., which handles credit reporting tasks for U.S. mobile telecommunications carrier T-Mobile US, Inc., was accessed without authorization, leading to the leak of subscriber information that included the social security numbers of 15 million individuals.** For more information, see the following T-Mobile US blog post, "T-Mobile CEO on Experian's Data Breach" (http://www.t-mobile.com/landing/experian-data-breach.html) and the Experian Information Solutions, Inc. website, "Overview: Unauthorized Acquisition of Personal Information" (http://www.experian.com/data-breach/t-mobilefacts.html).

S **5th: It was determined that the Seoul Metro in South Korea had been accessed without authorization in July 2014, resulting in a number of PCs including servers being infected with malware.**

S **5th: The official website of Taiji-cho in Wakayama Prefecture was targeted in DDoS attacks by Anonymous, temporarily rendering it inaccessible (OpKillingBay).**

O **6th: The JPCERT Coordination Center published a summary explaining and providing countermeasures for the Cross-Site Request Forgery (CSRF) Web application vulnerability that causes legitimate users to carry out unintended actions via malicious websites.** "Cross-Site Request Forgery (CSRF) and its Countermeasures" (http://www.jpcert.or.jp/securecoding/materials-csrf.html) (in Japanese).

S **10th: The official websites of Narita International Airport and Chubu Centrair International Airport were targeted in DDoS attacks by Anonymous, temporarily rendering them inaccessible (OpKillingBay).**

S **13th: The U.S. Federal Bureau of Investigation (FBI) and the U.K. National Crime Agency (NCA) jointly shut down a number of C&C servers for the Bugat (DRIDEX/CRIDEX) malware that targets online banking accounts, etc.** See the following Federal Bureau of Investigation statement for more information. "Bugat Botnet Administrator Arrested and Malware Disabled" (https://www.fbi.gov/pittsburgh/press-releases/2015/bugat-botnet-administrator-arrested-and-malware-disabled).

V **14th: Microsoft published their Security Bulletin Summary for October 2015, and released a total of six updates, including three critical updates such as MS15-106 and MS15-108, as well as three important updates.** "Microsoft Security Bulletin Summary for October 2015" (https://technet.microsoft.com/en-us/library/security/ms15-oct).

V **14th: A number of vulnerabilities in Adobe Flash Player that could allow unauthorized termination or arbitrary code execution were discovered and fixed.** "APSB15-25: Security updates available for Adobe Flash Player" (https://helpx.adobe.com/security/products/flash-player/apsb15-25.html).

V **14th: A number of vulnerabilities in Adobe Reader and Acrobat that could allow unauthorized termination and arbitrary code execution were discovered and fixed.** "Security Updates Available for Adobe Acrobat and Reader" (https://helpx.adobe.com/security/products/reader/apsb15-24.html).

V **15th: A vulnerability (CVE-2015-7645) in Adobe Flash Player that could allow unauthorized termination and arbitrary code execution was disclosed. A fix for this vulnerability was released on October 17.** "APSA15-05: Security Advisory for Adobe Flash Player" (https://helpx.adobe.com/security/products/flash-player/apsa15-05.html).

V **17th: A number of vulnerabilities in Adobe Flash Player that could allow unauthorized termination or arbitrary code execution were discovered and fixed.** "APSB15-27: Security updates available for Adobe Flash Player" (https://helpx.adobe.com/security/products/flash-player/apsb15-27.html).

V **19th: Oracle released their quarterly scheduled update for a number of products including Oracle, fixing a total of 154 vulnerabilities, including 25 in Java SE.** "Oracle Critical Patch Update Advisory - October 2015" (http://www.oracle.com/technetwork/topics/security/cpuoct2015-2367953.html).

O **20th: The National Institute of Information Communications Technology (NICT) published the results of their security evaluation of cryptographic protocols in list form. This was aimed at enabling system designers to use the cryptographic protocols appropriate for their intended purpose, and it covered 51 standardized cryptographic protocols, as well as seven other typical cryptographic protocols.** "List of Security Evaluation Results for Cryptographic Protocols Published" (http://www.nict.go.jp/press/2015/10/20-2.html) (in Japanese).

V **22nd: A vulnerability (CVE2015-7871) in ntpd that could allow system time settings to be manipulated by bypassing authentication through the receipt of malicious packets was discovered and fixed, along with a number of other vulnerabilities such as those that could enable abnormal server termination via specially-crafted packets.** "October 2015 NTP-4.2.8p4 Security Vulnerability Announcement (Medium)" (http://support.ntp.org/bin/view/Main/SecurityNotice#October_2015_NTP_4_2_8p4_Securit).

V **30th: A vulnerability in the router products of a number of manufacturers that could allow unintended router operations when users logged into the device accessed a specially-crafted page was discovered and fixed.** "JVN#48135658: Multiple routers contain issue in preventing clickjacking attacks" (http://jvn.jp/en/jp/JVN48135658/).

O **30th: The Information-technology Promotion Agency, Japan (IPA) issued a warning due to an increase in consultations about suspicious emails with Word document files attached that were presented as notices regarding orders or automatic messages from multi-function printers.** "[Alert] Beware of mass-sent emails presented as notices regarding orders from certain organizations" (http://www.ipa.go.jp/security/topics/alert271009.html) (in Japanese).

*Dates are in Japan Standard Time

Legend										
	V	Vulnerabilities	S	Security Incidents	P	Political and Social Situation	H	History	O	Other

code execution were discovered and fixed in the VMware virtual machine environment construction software[*16]. A vulnerability that could allow password protection to be disabled by simply pressing the backspace key repeatedly was discovered and fixed in the GRUB2 boot loader widely adopted on Linux[*17].

Regarding Android, a vulnerability (Stagefright 2.0) that could allow arbitrary code execution via specially-crafted files was discovered and fixed. It was identified that the Moplus software development kit (SDK) for Android apps had a vulnerability called Wormhole[*18] as well as a flaw that could allow attackers to read and control data on devices remotely, and these were fixed. In relation to this, a vulnerability that cloud allow malicious third parties to read data on devices was also discovered and fixed in another SDK (Push SDK)[*19].

As for industrial control systems, a number of vulnerabilities related to password processing were discovered and fixed in Omron-brand PLCs and the CX-Programmer software for programming them. These could have allowed passwords to be obtained when intercepted over communication routes due to the fact they were sent as plain text or taken from files on a system[*20]. Regarding products from domestic manufacturers, in September a vulnerability that could allow DoS attacks was discovered and fixed in Mitsubishi Electric brand MELSEC FX-series control system sequencers[*21]. Because industrial control systems are often used in closed environments, up until now it has been common for issues to be left unresolved for some time. However, in recent years there has been an increase in attacks targeting these systems, and it is becoming necessary to take measures such as checking vulnerability and attack information regularly, just as with conventional software[*22].

■ DDoS Attacks

A number of large-scale DDoS attacks occurred during this period. From around May 2015, DDoS attacks accompanied by threats from a group calling themselves DD4BC have been made on financial institutions and other parties. Since November, there have also been a number of DDoS attacks carried out by other groups. Among these, Swiss company Proton Technologies was threatened during the course of attacks by a group calling themselves the Armada Collective[*23], who continued their attacks on the firm even after it gave in to demands for payment. This group has also made attacks on financial institutions and hosting services in various other countries, and are thought to be involved in an incident in which a U.K. hosting service was forced to suspend services[*24]. Attacks on hosting services also included a large-scale DDoS attack on U.S. company Linode that lasted 12 days. Besides these, in December there were attacks on multiple game-related servers such as those for Xbox LIVE, PSN, and EA by a group calling themselves the Phantom Squad.

■ Information Leaks Due to Unauthorized Access

During this survey period, there were ongoing incidents of large-scale leaks of data including customer information due to unauthorized access to corporate systems.

An incident occurred in which the internal servers of Experian, which handles credit reporting tasks for U.S. mobile telecommunications carrier T-Mobile, were accessed without authorization, and the personal information including names and

[*16] "VMSA-2015-0007.2 VMware vCenter and ESXi updates address critical security issues." (https://www.vmware.com/security/advisories/VMSA-2015-0007).

[*17] See the following explanation by the discoverer for more details. "Back to 28: Grub2 Authentication 0-Day" (http://hmarco.org/bugs/CVE-2015-8370-Grub2-authentication-bypass.html).

[*18] See the following WooYun.org page for more information about the vulnerability. "WooYun-2015-148406 Wormhole 虫洞漏洞总结报告 (附检测结果与测试脚本)" (http://www.wooyun.org/bugs/wooyun-2015-0148406) (in Chinese).

[*19] Baidu Japan Inc. provided fixes due to the fact that their apps used the corresponding SDK. "About 'Simeji Privacy Lock'" (http://www.baidu.jp/info/press/report/151113.html) (in Japanese).

[*20] "Advisory (ICSA-15-274-01) Omron Multiple Product Vulnerabilities" (https://ics-cert.us-cert.gov/advisories/ICSA-15-274-01)..

[*21] "Advisory (ICSA-15-146-01) Mitsubishi Electric MELSEC FX-Series Controllers Denial of Service" (https://ics-cert.us-cert.gov/advisories/ICSA-15-146-01).

[*22] U.S. ICS-CERT (https://ics-cert.us-cert.gov/) provides information on vulnerabilities in industrial control systems that can be used as reference. In Japan, IPA also provides user-oriented reports on control systems, as well as Japanese translations of ICS-CERT and ENISA reports. IPA, "Control System Security" (https://www.ipa.go.jp/security/controlsystem/) (in Japanese).

[*23] See the following Swiss governmental CERT team blog post for information on the Armada Collective. "Armada Collective blackmails Swiss Hosting Providers" (http://www.govcert.admin.ch/blog/14/armada-collective-blackmails-swiss-hosting-providers).

[*24] For more information, see the following announcement from Moonfruit who was targeted in the attacks. "DDoS attack update: 14/12/2015" (https://support.moonfruit.com/hc/en-us/articles/207109805-DDoS-attack-update-14-12-2015).

November Incidents

1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30

S **1st: A list summarizing the publically-available personal information of people who agree with certain opinions on Facebook was published, causing a stir due to privacy and defamation issues. The real name and work contact information of the individual who created the list was subsequently identified, and the list was deleted.**

S **4th: A junior high school student was arrested on suspicion of storing and supplying electromagnetic records of a computer virus, with claims he had malware such as Zeus and SpyEye in his possession for the purpose of sale. A number of junior high school and high school students were also charged with obtaining electromagnetic records of a computer virus for purchasing or receiving malware from the arrested junior high school student.**

S **4th: The ProtonMail encrypted email service provided by Swiss company Proton Technologies was targeted in a large-scale DDoS attack (over 100 Gbps) that was accompanied by threats. In this incident, 15 BTC (around 700,000 yen) was paid after consulting with other affected companies, but the attacks did not subside, and donations were solicited so that countermeasures could be implemented.**
See the following article for more information, "ProtonMail Statement about the DDOS Attack"
(https://protonmaildotcom.wordpress.com/2015/11/05/protonmail-statement-about-the-ddos-attack/).

V **6th: A backdoor function in the Moplus software development kit (SDK) for Android apps was discovered and fixed.**
An investigation conducted by Trend Micro determined that at the time there were 14,112 apps with the Moplus SDK built in, including those with different versions and varying SHA-1 hash values. "Setting the Record Straight on Moplus SDK and the Wormhole Vulnerability"
(http://blog.trendmicro.com/trendlabs-security-intelligence/setting-the-record-straight-on-moplus-sdk-and-the-wormhole-vulnerability/).

S **10th: A man working for a communication equipment sales company was arrested by the Tokyo Metropolitan Police Department on suspicion of violating the Unauthorized Computer Access Law by using the ID and password of another person to access Facebook without authorization. This incident was came to light when a file containing a list of the Facebook and iCloud IDs and passwords for 771 individuals was discovered on the man's PC while investigating him on suspicion of public display of obscene images.**

V **11th: Microsoft published their Security Bulletin Summary for November 2015, and released a total of 12 updates, including four critical updates such as MS15-112 and MS15-115, as well as eight important updates.**
"Microsoft Security Bulletin Summary for November 2015" (https://technet.microsoft.com/library/security/ms15-nov).

V **11th: A number of vulnerabilities in Adobe Flash Player that could allow unauthorized termination or arbitrary code execution were discovered and fixed.**
"APSB15-28: Security updates available for Adobe Flash Player" (https://helpx.adobe.com/security/products/flash-player/apsb15-28.html).

S **16th: There was a string of incidents in which ads were unintentionally distributed via apps and update servers on a number of smartphones sold in Japan. For example, it was disclosed that in the case of the company ZTE this was due to a control error in the notification function for the app.**
"[Important notice] Apology regarding the mistaken distribution of ads to Blade S (g03) and Blade S Lite (g02)"
(http://www.zte.co.jp/products/handsets/sim_free/phone/info/201511/t20151117_445962.html) (in Japanese).

O **17th: The JPCERT Coordination Center published an explanation about utilizing and analyzing logs to deal with high-level cyber attacks such as targeted attacks.**
"Utilizing and analyzing logs when dealing with high-level cyber attacks" (http://www.jpcert.or.jp/research/apt-loganalysis.html) (in Japanese).

S **20th: The website of the Ministry of Health, Labour and Welfare was targeted in DDoS attacks by Anonymous, temporarily rendering it inaccessible (OpKillingBay). The website was unavailable between November 21 and November 23 due to these attacks.**
Ministry of Health, Labour and Welfare, "Ministry of Health, Labour and Welfare website available again"
(http://www.mhlw.go.jp/stf/houdou/0000104929.html) (in Japanese).

S **21st: It was discovered that customer data such as credit card information had been leaked due to PoS malware infections at over 50 Starwood-owned hotels in North America, including Sheraton and Westin locations.**
Starwood Hotels & Resorts Worldwide, Inc. "Letter From Our President - Updated"
(http://www.starwoodhotels.com/html/HTML_Blocks/Corporate/Confidential/Letter.htm?EM=VTY_CORP_PAYMENTCARDSECURITYNOTICE).

V **24th: It came to light that PCs had been shipped with root certificates pre-installed, and support tools provided by the manufacturer installed root certificates during software installation. Because the private key used to issue the certificates was included, this aroused much concern because it enabled third parties to create fraudulent sites and also made MITM attacks possible.**
See the following Dell blog post for more details. "Response to Concerns Regarding eDellroot Certificate"
(http://en.community.dell.com/dell-blogs/direct2dell/b/direct2dell/archive/2015/11/23/response-to-concerns-regarding-edellroot-certificate).

S **30th: Faults in the identity verification system specifications for a bank's balance inquiry call service were exploited, causing the leak of phone numbers input as the requestor's names when carrying out bank transfers.**
Bank of Tokyo-Mitsubishi UFJ, "Regarding the leak of phone numbers input as users on membership sites, etc."
(http://www.bk.mufg.jp/news/news2015/pdf/news1130.pdf) (in Japanese).

O **30th: Revisions were made to the "Guidelines for Dealing with Cyber Attacks and Privacy at Telecommunications Carriers - Fourth Version," which are designed to help telecommunications carriers legitimately identify and deal with communications such as DoS. The guidelines were then published by five telecommunications carrier organizations.**
"Revision to Guidelines for Dealing with Cyber Attacks and Privacy at Telecommunications Carriers"
(https://www.jaipa.or.jp/topics/2015/11/post.php) (in Japanese).

*Dates are in Japan Standard Time

Legend V Vulnerabilities S Security Incidents P Political and Social Situation H History O Other social security numbers for 15 million individuals may have leaked. The website of U.K. communications company TalkTalk was also accessed without authorization via an SQL injection attack, leading to the potential leak of information on 4 million subscribers. In relation to these incidents, a party threatened to publish leaked customer data unless a bitcoin payment was made*[25], and a 15-year-old boy was later arrested on suspicion of misuse of a computer. It has been identified that this incident was caused by an XSS vulnerability on the website*[26]. It was announced that U.S. online stock brokerage firm Scottrade had also been accessed without authorization, leading to the leak of information on around 4.6 million individuals*[27]. In another incident, personal information including password data for 480,000 vBulletin.com users leaked after an unpatched vulnerability in the vBulletin online forum software was exploited. This vulnerability was fixed swiftly, but it has been pointed out that many attacks may occur due to the disclosure of PoC code*[28]. Additionally, measures were taken after it came to light that 3.3 million pieces of user data had been mistakenly published on a community site for fans of Japanese characters*[29], and it was also discovered that the personal information of 190 million voters in the U.S. has been exposed*[30]. Security researchers have identified that these two incidents were caused by misconfigurations of servers that allowed third parties to access them.

■ Other

In October, it was disclosed that customer credit card information may have leaked from the Trump Hotel Collection due to unauthorized access to the internal system via malware infection. Hotel information leaks included the leak of customer data such as credit card information due to PoS malware infections at over 50 Starwood-owned hotels in North America in November. Additionally, in December payment information such as credit card data may have leaked at Hyatt Hotels due to a malware infection in their payment processing system. As these examples demonstrate, there have been a string of customer information leaks affecting mainly major hotel chains in the United States due to PoS malware infections. The affected hotels included those with operations in Japan.

In Japan, there was a series of incidents at a number of local public bodies in which resident information or voter data was taken by staff members or leaked. The reasons for these incidents vary, but material or data was taken, for example by copying it, in violation of internal regulations. In one incident in Miura City, Kanagawa Prefecture, it was discovered that a staff member had taken home a total of around two million files on a USB flash drive and stored the files there, including administrative documents containing the personal information of citizens*[31]. At Nishihara Village in the Aso District of Kumamoto Prefecture, it came to light that a staff member had copied to a PC or HDD and taken away over 180,000 pieces of personal information, including basic resident register data for everyone in the village*[32]. It was announced that no transfers to third parties or external leaks were confirmed in these incidents. In Sakai City, Osaka Prefecture, it was announced that files including the voter information of around 680,000 individuals had leaked to third parties, after a staff member took this data home and made it available on an external server they had signed up for*[33]. The staff member in question received a disciplinary dismissal due to this incident.

A junior high school student was arrested on suspicion of storing and supplying electromagnetic records of a computer virus, with claims he had malware such as Zeus and SpyEye in his possession for the purpose of sale. It was reported that the arrested junior

*25 KrebsOnSecurity, “TalkTalk Hackers Demanded £80K in Bitcoin” (http://krebsonsecurity.com/2015/10/talktalk-hackers-demanded-80k-in-bitcoin/).

*26 “video.talktalk.co.uk Security Vulnerability” (https://www.xssposed.org/incidents/93183/).

*27 Scottrade, Inc., “Cyber Security Update” (https://about.scottrade.com/updates/cybersecurity.html).

*28 For example, the following alert was issued on the official Symantec blog due to an increase in exploitation attempts. “Patch now! Cybercriminals are actively searching for servers running vulnerable versions of vBulletin” (http://www.symantec.com/connect/tr/blogs/patch-now-cybercriminals-are-actively-searching-servers-running-vulnerable-versions-vbulletin).

*29 “Regarding reports of a vulnerability on a Sanrio character site run by a Hong Kong company” (http://www.sanrio.co.jp/wp-content/uploads/2015/05/20151224.pdf) (in Japanese).

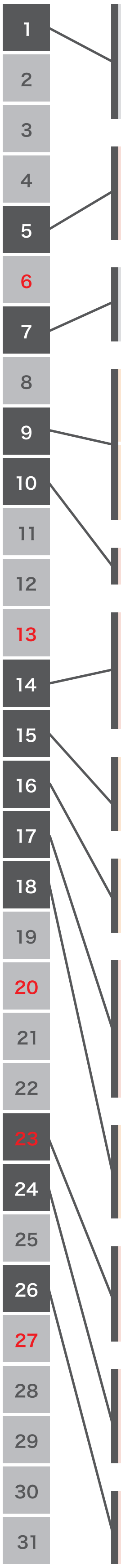
*30 See the following DataBreaches.net article for more information. “191 million voters’ personal info exposed by misconfigured database (UPDATE2)” (http://www.databreaches.net/191-million-voters-personal-info-exposed-by-misconfigured-database/).

*31 Miura, Kanagawa Prefecture, “Apology and report on the unauthorized removal of administrative documents by a city staff member” (http://www.city.miura.kanagawa.jp/hisho/press/2015/documents/151002info.pdf) (in Japanese).

*32 Nishihara, Aso District, Kumamoto Prefecture, “Regarding the improper handling of administrative information (report and additional apology) (http://www.vill.nishihara.kumamoto.jp/oshirase/_2012.html) (in Japanese).

*33 Sakai, Osaka Prefecture, “Regarding our staff member’s impropriety” (http://www.city.sakai.lg.jp/shisei/koho/hodo/hodoteikyoshiryo/kakohodo/teikyoshiryo_h27/teikyoshiryo_h2712/1214_02.files/1214_02.pdf) (in Japanese).

December Incidents



O **1st: BlackBerry revealed they had received a request from the government of Pakistan to make the monitoring of emails and messages possible, and announced they would withdraw their business from Pakistan at the end of 2015 due to unwillingness to fulfill that request.**
See the following BlackBerry blog post for more information. "Why BlackBerry is Exiting Pakistan (Updated Dec 31)" (http://blogs.blackberry.com/2015/11/why-blackberry-is-exiting-pakistan/). They later announced they would continue operations after negotiations with the government of Pakistan. "Continuing our Operations in Pakistan" (http://blogs.blackberry.com/2015/12/continuing-our-operations-in-pakistan/).

S **5th: A series of cases involving infection with ransomware (malware that encrypts files and holds them ransom) that encrypted files and changed their extensions to ".vvv" attracted attention.**
See the following Tokyo SOC Report from IBM for more information. "Attacks aimed at infecting users with the CryptoWall ransomware confirmed on successive days from late November" (https://www-304.ibm.com/connections/blogs/tokyo-soc/entry/ransomware_20151208?lang=ja) (in Japanese).

O **7th: The National center of Incident readiness and Strategy for Cybersecurity held an intersectoral exercise for critical infrastructure.**
"Summary of Intersectoral Exercise for Critical Infrastructure [2015 Annual Intersectoral Exercise]" (http://www.nisc.go.jp/active/infra/pdf/bunya_enshu2015gaiyou.pdf) (in Japanese).

V **9th: Microsoft published their Security Bulletin Summary for December 2015, and released a total of 12 updates, including eight critical updates such as MS15-124 and MS15-131, as well as four important updates including MS15-135.**
"Microsoft Security Bulletin Summary for December 2015" (https://technet.microsoft.com/en-us/library/security/ms15-dec).

V **9th: A number of vulnerabilities in Adobe Flash Player that could allow unauthorized termination or arbitrary code execution were discovered and fixed.**
"APSB15-32: Security updates available for Adobe Flash Player" (https://helpx.adobe.com/security/products/flash-player/apsb15-32.html).

S **10th: The personal website of Prime Minister Abe was targeted in DDoS attacks by Anonymous, temporarily rendering it inaccessible (OpKillingBay).**

S **14th: NIC.tr, the ccTLD registrar for Turkey's .tr domains, was targeted in a large-scale DDoS attack that prevented name resolution, among other effects. It is thought that requests from overseas were temporarily filtered to deal with this attack. These attacks also causes delays, etc., at the RIPE Network Coordination Center that serves as a secondary DNS.**
See the following NIC.tr report for more information. "14/12/2015 Tarihinde Başlayan DDoS Saldırısı" (https://www.nic.tr/2015-12-DDoS-Saldirisi-Kamuoyu-Duyurusu-20151221.pdf) (in Turkish).

V **15th: A number of vulnerabilities in Joomla! were discovered and fixed, including the CVE-2015-8562 that could allow remote code execution by a third party.**
"Joomla! 3.4.6 Released" (https://www.joomla.org/announcements/release-news/5641-joomla-3-4-6-released.html).

V **16th: Multiple vulnerabilities in BIND9 were discovered and fixed, included those that could allow attackers to perform DoS attacks by requesting records with malformed class attributes.**
Internet Systems Consortium, "BIND 9 Security Vulnerability Matrix" (https://kb.isc.org/article/AA-00913/).

S **17th: In Brazil, a court order was issued to block the WhatsApp application due to WhatsApp ignoring a court order, resulting in it being temporarily blocked by telecommunications companies.**
See the following statement from a court in the state of São Paolo for more information on the court order. "16/12/2015 - Justiça determina bloqueio do aplicativo WhatsApp" (http://www.tjsp.jus.br/Institucional/CanaisComunicacao/Noticias/Noticia.aspx?Id=29056) (in Portuguese). This decision called for a 48-hour suspension, but it was withdrawn and the block removed after about 12 hours. "17/12/2015 - TJSP CONCEDE LIMINAR PARA RESTABELECER WHATSAPP" (http://www.tjsp.jus.br/Institucional/CanaisComunicacao/Noticias/Noticia.aspx?Id=29057) (in Portuguese).

V **18th: Juniper Networks, Inc. issued a fix for a vulnerability it had found in ScreenOS that could allow remote access with administrator privileges, as well as a vulnerability that could allow decryption of VPN communications.**
"2015-12 Out of Cycle Security Bulletin: ScreenOS: Multiple Security issues with ScreenOS (CVE-2015-7755, CVE-2015-7756)" (http://kb.juniper.net/InfoCenter/index?page=content&id=JSA10713&actp=search).

S **23rd: It was announced that there was a vulnerability in a community site for fans of Japanese characters that made it possible to view personal information registered there.**
"Security Advisory: Corrected a vulnerability involving personal information of SanrioTown.com members" (http://blog.sanriotown.com/blog/2015/12/22/security-advisory-corrected-a-vulnerability-involving-personal-information-of-sanriotowncom-members/).

S **24th: At a number of power distribution companies in Ukraine, substation systems were accessed without authorization due to malware infections, leading to large-scale power outages.**
See the following SANS Industrial Control Systems Security Blog post for more information. "Confirmation of a Coordinated Attack on the Ukrainian Power Grid" (https://ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid).

S **26th: Large-scale DDoS attacks lasting 12 days were made on U.S. hosting provider Linode.**
See the following Linode blog post for more information on these attacks. "The Twelve Days of Crisis - A Retrospective on Linode's Holiday DDoS Attacks" (https://blog.linode.com/2016/01/29/christmas-ddos-retrospective/).

*Dates are in Japan Standard Time

Legend V **Vulnerabilities** S **Security Incidents** P **Political and Social Situation** H **History** O **Other**

high school student obtained these malware creation toolkits from overseas Internet sites. A number of junior high school and high school students were also charged with obtaining electromagnetic records of a computer virus for purchasing or receiving malware from this junior high school student.

Also in November, in light of the Ministry of Internal Affairs and Communications' "Workshop on the Appropriate Way to Handle Cyber Attacks in the Telecommunications Business" issuing their second summary in September, the "Guidelines for Dealing with Cyber Attacks and Privacy at Telecommunications Carriers" that deal with the lawful implementation of these measures were amended, and published by five organizations related to the telecommunications business. These amendments provided new guidelines for issuing alerts to users and blocking communications with C&C servers, etc. Also see "1.4.3 Guidelines for Dealing with Cyber Attacks and Privacy at Telecommunications Carriers" for more information.

1.3 Incident Survey

1.3.1 DDoS Attacks

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

Direct Observations

Figure 2 shows the circumstances of DDoS attacks handled by the IIJ DDoS Protection Service between October 1 and December 31, 2015.

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

There are many methods that can be used to carry out a DDoS attack, and the capacity of the environment attacked (bandwidth and server performance) will largely determine the degree of impact. Figure 2 categorizes DDoS attacks into three types: attacks on bandwidth capacity[*34], attacks on servers[*35], 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 954 DDoS attacks. This averages to 10.37 attacks per day, indicating a dramatic increase in the average daily number of attacks compared to our prior report. This was due to the large-scale occurrence of attacks on specific targets, which accounted for 63.8% of the overall number of attacks. Server attacks accounted for 67.7% of all incidents, while compound attacks accounted for 30.7%, and bandwidth capacity attacks 1.6%.

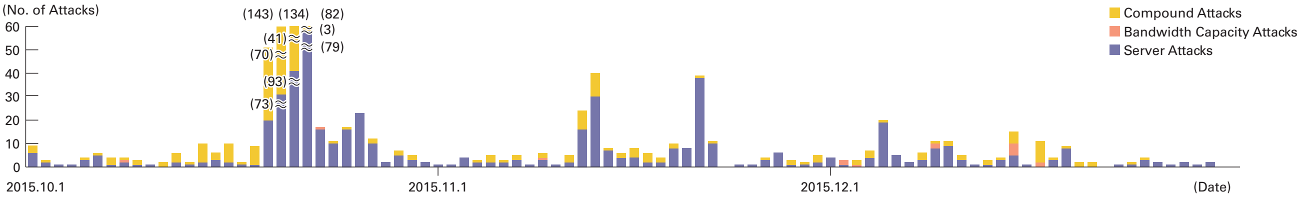


Figure 2: Trends in DDoS Attacks

*34 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.

*35 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.

The largest attack observed during the period under study was classified as a compound attack, and resulted in 2.87 Gbps of bandwidth using up to 1,202,000 pps packets.

Of all attacks, 89.6% ended within 30 minutes of commencement, 10.1% lasted between 30 minutes and 24 hours, and 0.3% lasted over 24 hours. The longest sustained attack for this period was a compound attack that lasted for one day, 14 hours, and 15 minutes (38 hours and 15 minutes).

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*[36] and botnet*[37] usage as the method for conducting DDoS attacks.

Backscatter Observations

Next we present our observations of DDoS attack backscatter using the honeypots*[38] set up by the MITF, a malware activity observation project operated by IIJ*[39]. By monitoring backscatter it is possible to detect some of the DDoS attacks occurring on external networks as a third party without any interposition.

For the backscatter observed between October 1 and December 31, 2015, Figure 3 shows the sender's IP addresses classified by country, and Figure 4 shows trends in packet numbers by port.

The port most commonly targeted by the DDoS attacks observed was the 53/UDP port used for DNS, accounting for 49.4% of the total. This was followed by 80/TCP used for Web services at 18.5%, so the top two ports accounted for 67.9% of the total. Attacks were also observed on 53/TCP used by DNS, 443/TCP used for HTTPS, 8080/TCP sometimes used for HTTP, and 27015/UDP that is sometimes used for game communications, as well as 53261/TCP and 3306/UDP, which are not commonly used.

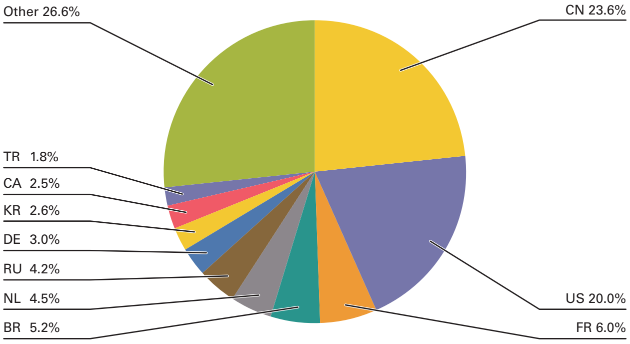


Figure 3: DDoS Attack Targets by Country According to Backscatter Observations

Examining the daily average number of packets for the 53/UDP communications observed often since February 2014, we can see that although it has dropped to 4,600 compared to around 5,800 in the previous survey period, it remains at a high level.

Looking at the origin of backscatter thought to indicate IP addresses targeted by DDoS by country in Figure 3, China accounted for the largest ratio at 23.6%. The United States and France followed at 20.0% and 6.0%, respectively.

Regarding particularly large number of backscatter packets observed by port, there were attacks on Web servers (80/TCP

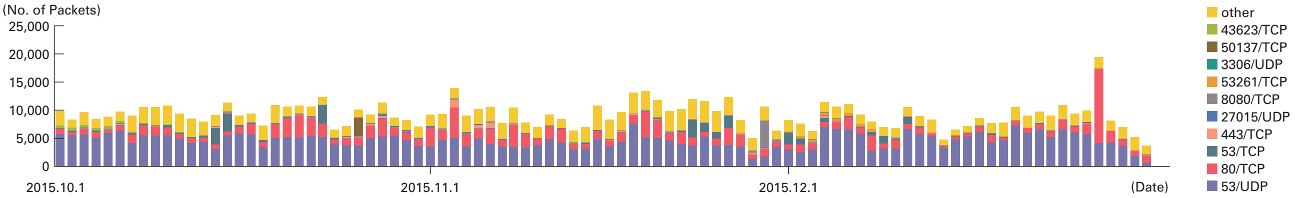


Figure 4: Observations of Backscatter Caused by DDoS Attacks (Observed Packets, Trends by Port)

*36 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 to make it appear as if the attack is coming from a different location, or from a large number of individuals.

*37 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.

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

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

and 443/TCP) thought to be related to ISIL between October 21 and November 6, as well as on November 13 and 18. Attacks on a U.S. online casino were also observed on November 3 and 6. There were also attacks on an online service platform for consumer game consoles between November 27 and 29, and attacks on the servers of a hosting provider in the Netherlands on December 27. Attacks on other ports included those targeting 53/TCP on a number of DNS servers for a U.S. CDN provider intermittently between October 14 and December 11. We also observed attacks on 8080/TCP, etc., targeting the servers of a French hosting provider between November 25 and 30.

Notable DDoS attacks during the current survey period that were detected via IIJ's observations of backscatter included attacks on a DNS server group for Turkish .tr domains between December 14 and 15, as well as attacks by Anonymous targeting the Turkish government and a number of banks on December 22 and 24. On December 31, attacks on a number of Web servers for a U.K. broadcaster were also detected.

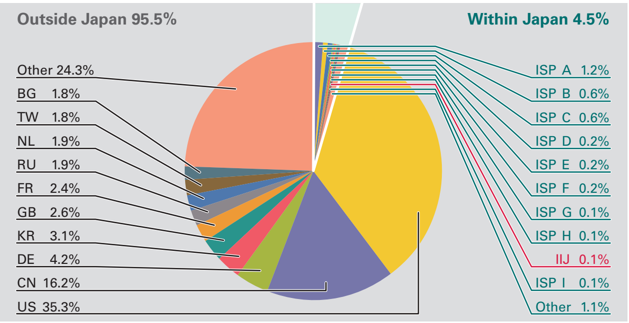


Figure 5: Sender Distribution

1.3.2 Malware Activities

Here, we will discuss the results of the observations of the MITF[*40], a malware activity observation project operated by IIJ. The MITF uses honeypots[*41] 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.

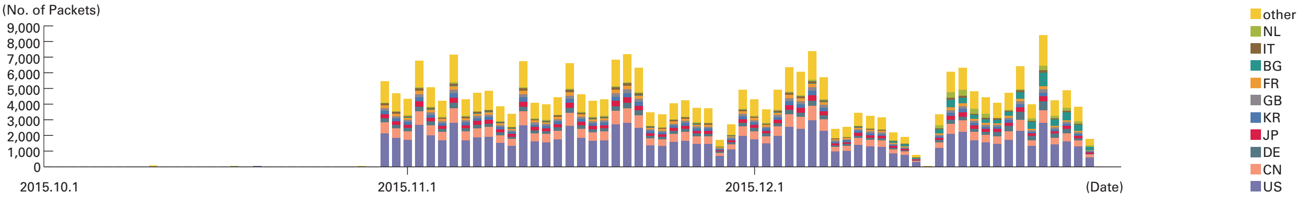


Figure 6: Communications Arriving at Honeypots (by Date, 53/UDP, per Honeypot)

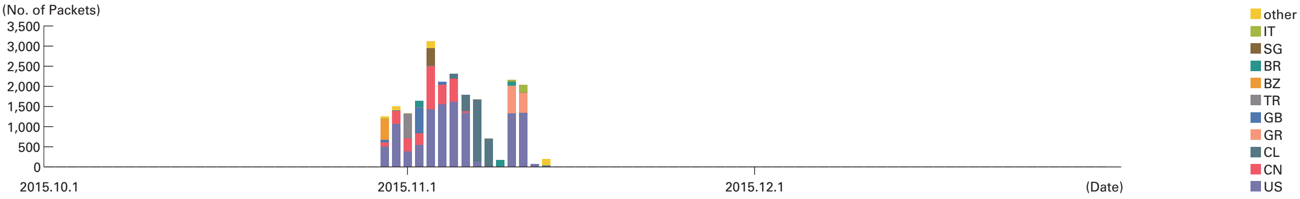


Figure 7: Communications Arriving at Honeypots (by Date, 1900/UDP, per Honeypot)

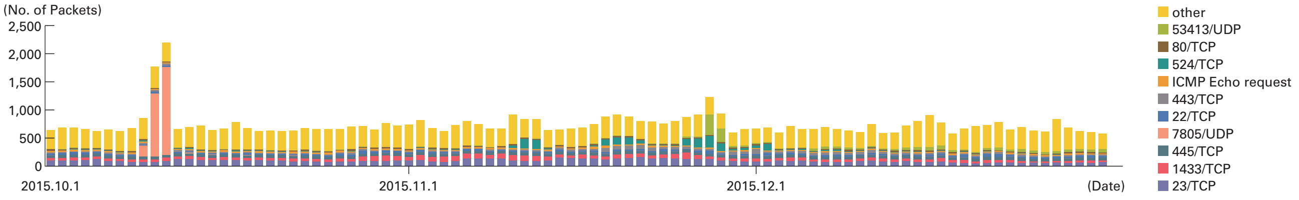


Figure 8: Communications Arriving at Honeypots (by Date, by Target Port, per Honeypot)

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

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

■ Status of Random Communications

Figure 5 shows the distribution of sender's IP addresses by country for communications coming into the honeypots between October 1 and December 31, 2015. Regarding the total volume (incoming packets), because the most prevalent and second most prevalent 53/UDP and 1900/UDP communications were significantly higher than other communications during the survey period for this report, we have plotted trends for them on Figure 6 and Figure 7, with other communications shown on Figure 8. The MITF has set up numerous honeypots for the purpose of observation. We have taken the average per honeypot, showing the trends by country in Figure 6 and Figure 7, and trends for incoming packet types (top ten) in Figure 8. Additionally, in these observations we corrected data to count multiple TCP connections as a single attack when the attack involved multiple connections to a specific port, such as attacks on MSRPC.

Much of the communications arriving at the honeypots during the current survey period targeted 53/UDP used by DNS, 1900/UDP used for the UPnP SSDP protocol, 23/TCP used for TELNET, 445/TCP used by Microsoft OSes, 1433/TCP used by Microsoft's SQL Server, 22/TCP used for SSH, 80/TCP and 443/TCP used by Web servers, ICMP echo requests, or 524/TCP used for the NetWare Core Protocol (NCP).

From October 30, there was a sharp rise in communications targeting 53/UDP. Upon investigating these communications, DNS name resolution requests from a range of source IP addresses allocated mainly to the United States and China were being repeatedly received on the IP address of a certain MITF honeypot. A number of corresponding domain names were also confirmed, and many were sites related to gambling, games, and science fiction novels in China. Because the majority of these communications involved repeated name resolution attempts for "(random).(existing domain)," we determined them to be DNS water torture attacks*[42].

Between October 30 and November 13, there was an increase in 1900/UDP communications for the SSDP protocol. We received SSDP search requests from IP addresses allocated mainly to countries such as the United States, China, Chile, and Greece. These communications are thought to have been searching for devices that could be used in DDoS attacks using SSDP reflectors.

Between October 9 and 11, there was an increase in 7805/UDP communications. An investigation revealed we had received concentrated name resolution return packets for multiple DNS names from a variety of source IP addresses.

Between November 27 and 28, there was an increase in 53423/UDP communications. We found that these were attacks targeting Netis and Netcore brand router vulnerabilities. These vulnerabilities were reported by Trend Micro in August 2014*[43], and JPCERT/CC announced there was a spike in attacks between April and June, 2015*[44].

■ Malware Network Activity

Figure 9 shows the distribution of the specimen acquisition source for malware during the period under study, while Figure 10 shows trends in the total number of malware specimens acquired. Figure 11 shows trends in the number of unique specimens. In Figure 10 and Figure 11, the trends in the number of acquired specimens show the total number of specimens acquired per day*[45], while the number of unique specimens is the number of specimen variants categorized according to their digest of a hash function*[46]. Specimens are also identified using anti-virus software, and a breakdown of the top 10 variants is displayed color coded by malware name. As with our previous report, for Figure 10 and Figure 11 we have detected Conficker using multiple anti-virus software packages, and removed any Conficker results when totaling data.

*42 Secure64 Software Corporation, "Water Torture: A Slow Drip DNS DDoS Attack" (https://blog.secure64.com/?p=377). For an explanation in Japanese, see the following document written by Mr. Yasuhiro Orange Morishita of Japan Registry Services. "DNS Water Torture Attacks" (http://2014.seccon.jp/dns/dns_water_torture.pdf) (in Japanese). The MITF honeypots do not query authoritative servers or cache servers when they receive DNS query packets, so they provide no aid to attacks.

*43 "Netis Routers Leave Wide Open Backdoor" (http://blog.trendmicro.com/trendlabs-security-intelligence/netis-routers-leave-wide-open-backdoor/)

*44 "Fixed Point Observation Report on the Internet (April to June, 2015)" (https://www.jpcert.or.jp/tsubame/report/report201504-06.html) (in Japanese).

*45 This indicates the malware acquired by honeypots.

*46 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.

On average, 73 specimens were acquired per day during the period under study, representing 15 different malware. After investigating the undetected specimens more closely, they included worms[*47] observed from IP addresses allocated to countries such as Taiwan, the United States, Mexico, and China.

About 55% of undetected specimens were in text format. Because many of these text format specimens were HTML 404 or 403 error responses from Web servers, we believe this was due to infection behavior of malware such as old worms continuing despite the closure of download sites that newly-infected PCs access to download malware. Under the MITF's independent analysis, during the current period under observation 85.7% of malware specimens acquired were worms, 1.4% were bots, and 12.9% were downloaders. In addition, the MITF confirmed the presence of seven botnet C&C servers[*48] and one malware distribution site.

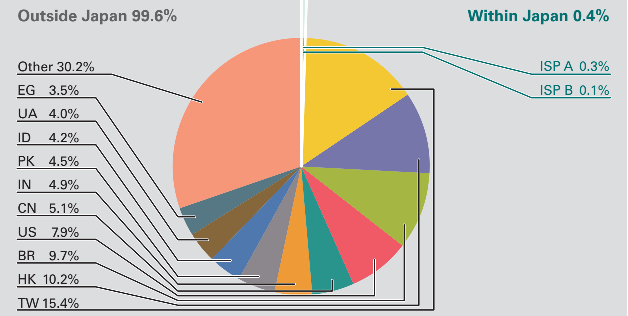


Figure 9: Distribution of Acquired Specimens by Source
(by Country, Entire Period under Study, Excluding Conficker)

Conficker Activity

Including Conficker, an average of 17,905 specimens were acquired per day during the period under study for this report, representing 480 different malware. Conficker accounted for 99.6% of the total specimens acquired, and 96.9% of the unique specimens. This demonstrates that Conficker remains the most prevalent malware by far, so we have omitted it from figures in this report. Compared to the previous survey period, the total number of specimens acquired decreased by approximately 36% during the period covered by this report, and the number of unique specimens decreased by about 12%. As reported in the previous volume, this is because infection activity from IP

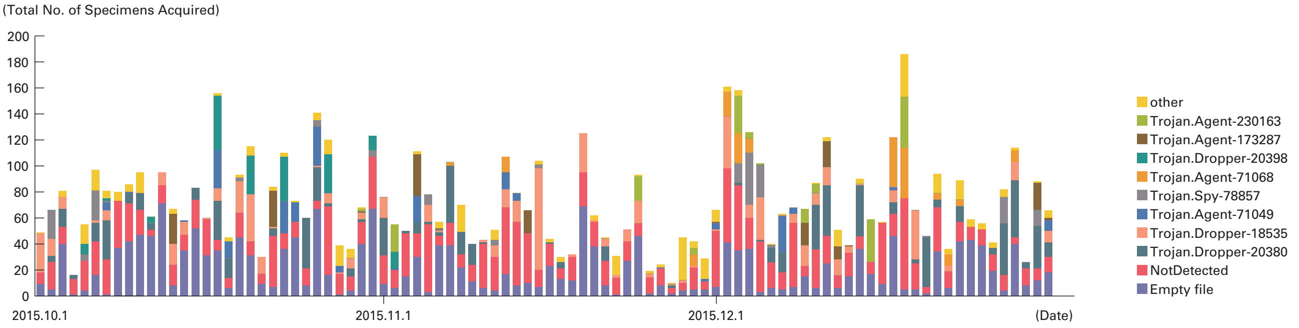


Figure 10: Trends in the Total Number of Malware Specimens Acquired (Excluding Conficker)

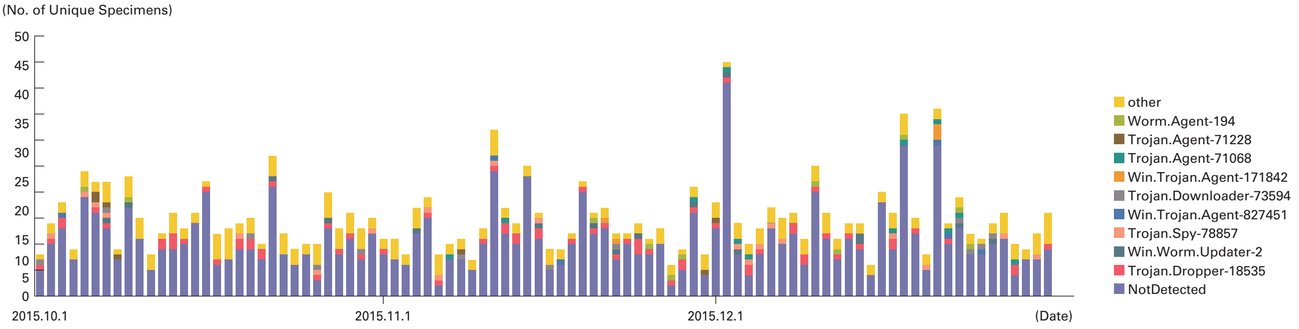


Figure 11: Trends in the Number of Unique Specimens (Excluding Conficker)

[*47] Worm: Win32/Dipasik.A (https://www.microsoft.com/security/portal/threat/encyclopedia/entry.aspx?Name=Worm:Win32/Dipasik.A).

[*48] An abbreviation of Command & Control Server. A server that provides commands to a botnet consisting of a large number of bots.

addresses allocated to the United States that spiked in July was no longer observed after August. According to the observations of the Conficker Working Group*[49], as of January 1, 2016, a total of 426,262 unique IP addresses are infected. This indicates a drop to about 13% of the 3.2 million PCs observed in November 2011, but it demonstrates that infections are still widespread.

1.3.3 SQL Injection Attacks

Of the types of different Web server attacks, IIJ conducts ongoing surveys related to SQL injection attacks*[50]. 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 12 shows the distribution of SQL injection attacks against Web servers detected between October 1 and December 31, 2015. Figure 13 shows trends in the numbers of attacks. These are a summary of attacks detected by signatures on the IIJ Managed IPS/IDS Service. China was the source for 35.4% of attacks observed, while the United States and Japan accounted for 25.2% and 17.9%, respectively, with other countries following in order. A greater number of SQL injection attacks against Web servers occurred compared to the previous report.

During this period, attacks from a specific attack source in the United States directed at specific targets took place on October 10. Between October 12 and 13, attacks were made from a specific attack source in China against specific targets. This attack source also carried out attacks on another specific target on November 3. On November 8, there were attacks from specific attack sources in Israel directed at specific targets. On November 12, there were attacks from specific attack sources in Canada directed at specific targets. These attacks are thought to have been attempts to find vulnerabilities on Web servers.

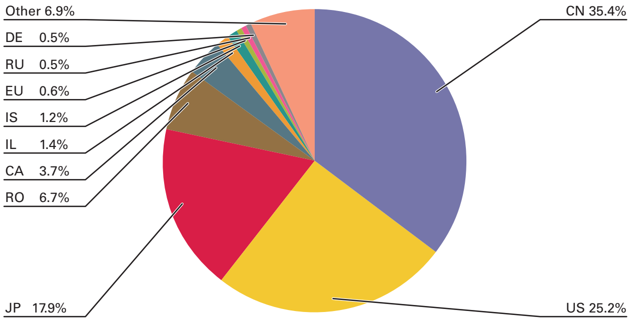


Figure 12: Distribution of SQL Injection Attacks by Source

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.

1.3.4 Website Alterations

Here we indicate the status of website alterations as surveyed through the MITF Web crawler (client honeypot)*[51].

This Web crawler accesses hundreds of thousands of websites on a daily basis, with a focus on well-known and popular sites in Japan. In addition to this, we temporarily monitor websites

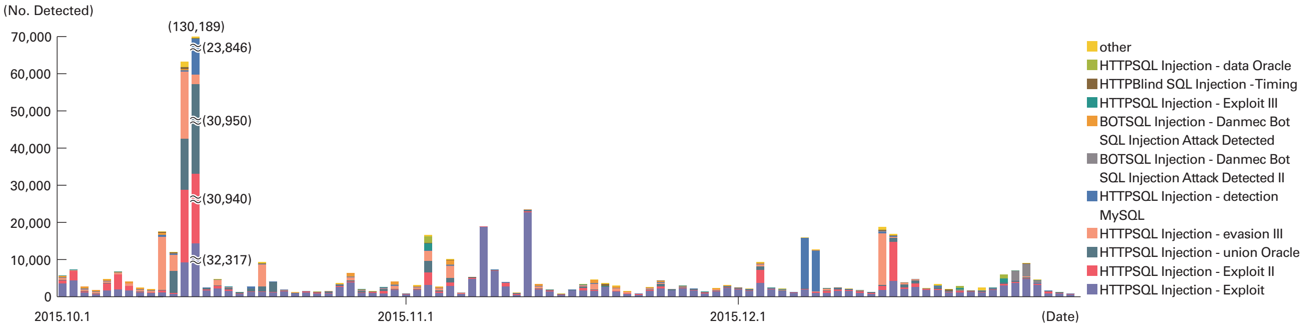


Figure 13: Trends in SQL Injection Attacks (by Day, by Attack Type)

*49 Conficker Working Group Observations (http://www.confickerworkinggroup.org/wiki/pmwiki.php/ANY/InfectionTracking).

*50 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.

*51 See "1.4.3 Website Defacement Surveys Using Web Crawlers" in Vol.22 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol22_EN.pdf) for an explanation of Web crawler observation methods.

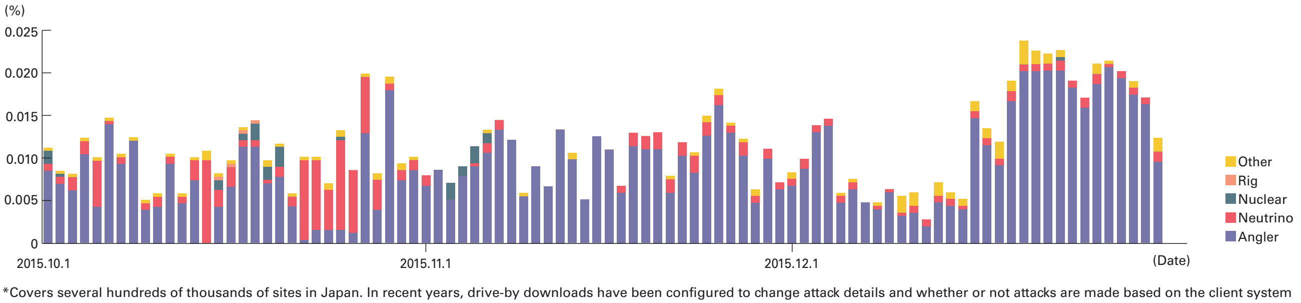
that have seen short-term increases in access numbers. By surveying websites thought to be viewed frequently by typical users in Japan, it is easier to speculate on trends regarding fluctuations in the number of altered sites, as well as the vulnerabilities exploited and malware distributed.

For the period between October 1 and December 31, 2015, Angler accounted for the majority of drive-by download attacks detected (Figure 14)*[52]. This trend has been consistent since around July. The total number of drive-by download attacks was about 40% higher than the total number for July to September. Additionally, in late October, some of the attackers that had up that point used Angler switched to using Neutrino. Subsequently, in November almost all attacks were once again using Angler. It appears that attackers temporarily changed tools for some reason. Changes thought to indicate a similar switch of tools before switching back were also observed intermittently a total of three times in August and September. During the current survey period, attacks via Nuclear and Rig were also observed, but each of these was small in scale.

The majority of malware downloaded was CryptoWall 3.0/4.0. In October, TeslaCrypt 2.0/2.2 was also confirmed in small numbers, but after November TeslaCrypt was no longer observed. Downloads of Necurs, Bedep, and Tinba have also been confirmed. Additionally, we saw multiple cases in which users redirected to exploit kits through website alterations or malvertising were routed via open redirectors during the transition. We speculate that this was intended to spoof the direct redirection source for the infector, and block analysis of changes to identify attacks by deleting the Referrer header recorded by proxy servers, etc., using an HTTPS redirector.

Additionally, after late November a large number of cases were observed in which users were redirected to fraudulent sites that displayed screens in the browser made to appear like Windows blue screen errors to suggest a malware infection has occurred. These sites also displayed a warning in a pop-up window that prompted users to phone a number purporting to be technical support. A number of domains previously used for some kind of service were reacquired after lapsing and exploited as gateways for the redirection of users to these fraudulent sites*[53].

An extremely high number of drive-by download attacks continue to occur. Website operators must take measures to prevent the alteration of Web content, and properly manage the mashup content provided by external third parties, such as advertisements and Web analytics services. We recommend that they stay aware of the security policies and reputations of content providers. When making externally accessible redirectors publically available, you must be aware of the potential for them to be exploited in link laundering as mentioned previously. It is important for browser users and administrators to check for vulnerabilities in OSes and browser-related plug-ins, and carry out thorough countermeasures such as applying updates and implementing EMET.



*Covers several hundreds of thousands of sites in Japan. In recent years, drive-by downloads have been configured to change attack details and whether or not attacks are made based on the client system environment or session information, source address attributes, and the quota achievement status of factors such as number of attacks. This means that results can vary wildly at times depending on the test environment and circumstances.

Figure 14: Rate of Drive-By Download Incidence When Viewing Websites (%) (by Exploit Kit)

*52 See "1.4.2 Angler Exploit Kit on the Rampage" in Vol.28 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol28_EN.pdf) for more information about our observations of the status and functions of Angler in July 2015.

*53 See "Alert regarding fraudulent sites that display ISP information and redirect users to fake support desks" (https://sect.iij.ad.jp/d/2015/12/258504.html) (in Japanese) from our Security Diary for more information on similar fraudulent sites.

1.4 Focused Research

Incidents occurring over the Internet change in type and scope from one minute to the next. Accordingly, IIJ works toward implementing countermeasures by continuing to perform independent surveys and analyses of prevalent incidents. Here, we present information from the surveys we have undertaken during this period regarding international standards for cloud security, as well as the Let's Encrypt project and the ACME protocol for automatically issuing certificates. We also discuss the Guidelines for Dealing with Cyber Attacks and Privacy at Telecommunications Carriers.

1.4.1 International Standards for Cloud Security

10 years have already passed since the concept of cloud computing was proposed by Google in 2006. Initially, a variety of discussion arose regarding aspects such as its definition, and there were many organizations that postponed adoption of it due to security concerns. However, there is now wide general recognition of cloud computing, and it is accepted as indispensable.

That said, when an organization actually makes moves to use a cloud service, security issues are still the greatest concern. Cloud service providers (hereinafter "providers") have implemented security measures to dispel these concerns, but as the measures taken by each company vary, users of cloud services (hereinafter "users") have a difficult time comparing and determining which service is more secure. It is also true that considerable effort is required to use cloud services.

International standards regarding the security management of cloud services have been examined as a method for resolving issues such as these, and in December 2015, ISO/IEC 27017:2015 (hereinafter "ISO 27017") was published. Here we will discuss points for utilizing ISO 27017.

■ Background to the Development of ISO 27017

■ Cloud Service Characteristics

Before examining ISO 27017, let us reflect on the characteristics of cloud services. Cloud services are fixed services for which no customization is carried out. When providing services, providers create cost and scale benefits through a variety of means, such as cutting elements requiring human intervention and performing automation, as well as consolidating and sharing equipment and operational structures to use resources efficiently. Consequently, cloud services make it intrinsically difficult to provide individual manual support and disclose internal system information. It is necessary to understand that this is a characteristic of cloud services.

This characteristic makes it hard for users to manage security. Managing information on your own organization requires detailed knowledge of management status, namely who handles internal information and in what manner. However, unlike discrete system development where your organization's security policies are applied, it is not possible to apply the security policies of a specific organization to cloud services in which resources are shared. For this reason, users sign up and use cloud services without verifying the security measures claimed by the provider themselves, under the assumption that the provider will not disclose security management details.

■ Development of ISO 27017

A gap exists between users and providers with regard to security management on cloud services such as those mentioned above, and a variety of methods have been devised to close this gap. We discussed one of these, a cloud information security audit system by the Cloud Information Security Promotion Alliance, in Vol.24 of this report*54. Using various security standards to confirm the security of a cloud service makes it easy for users to ascertain the extent that a provider conforms to security standards, and it also allows providers to easily indicate the level of their security measures, so this method has mutual benefits. In light of this, a range of standards, guidelines, and certification systems have been created by related organizations and groups both in Japan and overseas. However, this has resulted in there being a large number of independent standards, which undeniably has the reverse effect of causing confusion among providers and users. The international unification of cloud security management standards has now become essential.

*54 IIR Vol.24 "1.4.3 Cloud Security Confirmation and Audit Systems" (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol24_EN.pdf).

Under such conditions, the Ministry of Economy, Trade and Industry issued cloud security guidelines in Japan ahead of the rest of the world*55. ISO 27017 discussions began based on the guidelines issued by the ministry, so it could be said Japan played an extremely important role in developing these international standards. In addition to countries such as the U.S. and U.K., organizations such as the Cloud Security Alliance also participated in the formulation process, and many discussions took place. ISO 27017 has a slightly complex structure, as it incorporates a variety of opinions from people with different perspectives, such as regions and countries centered around providing services, and conversely regions and countries centered around using services, as well as those with their own security standards. Next, we will take a look at a number of points to understand about ISO 27017.

■ Points to Understand About ISO 27017

■ Different Perspectives for Use

To reiterate, users determine and select the cloud services that meet the requirements of their organization from among services whose specifications have been set by the provider. This is the basic idea behind ISO 27017, which contains details that pertain to both users and providers. When applying ISO 27017, to avoid confusion it is important to properly understand whether you are conforming to these standards from the perspective of a provider, a user, or both.

Accordingly, it is necessary to clarify the scope of responsibility for providers and users. This indicates what control measures should be carried out in terms of an organization’s scope of responsibility. Consequently, a shared responsibility item has been added to ISO 27017 to clearly distinguish what security management tasks are assigned to the user and the provider, and how they should be carried out.

Providers that offer SaaS using IaaS are also users at the same time. Therefore, for services like this they would conform from the perspective of both user and provider.

■ Chapters and Organization

ISO 27017 is a set of controls that supplement ISO/IEC 27002:2013 (hereinafter “ISO 27002”), and the controls listed in each chapter match the numbers in ISO 27002. For this reason, in cases where ISO 27002 can be applied as-is, “ISO/IEC 27002 apply.” is listed. In other words, an organization must have implemented ISMS to comply with these standards.

To begin with, ISO 27002 is positioned as a guide for implementing ISO 27001, and it describes in specific terms how organizations should carry out security management themselves. It is not meant to determine the nature of security controls for services that providers offer. Accordingly, as ISO 27017 is based on ISO 27002, the basic idea behind it is also how users can carry out security management themselves. Another easy to understand way of looking at it is that it is revised from the perspective of determining how cloud service providers should meet the needs of cloud service users.

Its actual content includes “implementation guidance” as considerations specific to cloud computing. This implementation guidance is presented in table form, separated into tasks that should be implemented by users, and those that should be implemented by providers. When tasks are carried out by both parties, tables are merged. Aside from implementation guidance, points that should be taken into consideration and items requiring special mention are listed as “other information.”

Furthermore, controls specific to cloud services that do not exist in ISO 27001 are defined in ISO 27017. Specific examples include controls regarding improving the security of virtual environments, and controls associated with erasing information assets. These cloud-specific controls are not listed in the main text, but in Annex A numbered CLD x.y.z, so take care not to omit these from your considerations.

■ Utilization

Here we will explain how to use these standards. Regarding utilization by users, for those using cloud services in their organization, they would implement the “cloud service customer” items listed under “implementation guidance.” As touched upon previously,

[*55] Ministry of Economy, Trade and Industry, “Information security management guidelines for the use of cloud computing services - 2013 edition” (http://www.meti.go.jp/press/2013/03/20140314004/20140314004-2.pdf) (in Japanese).

ISO 27017 describes additional measures an organization compliant with ISMS should carry out to use cloud services, so when ISMS security management has not been implemented, note that it is necessary to start there.

Meanwhile, providers would refer to the “cloud service provider” items listed under “implementation guidance,” and implement the information to provide to users and security functions that should be in place on systems. Because there are some elements that need to be implemented as service functions in advance, such as log management and systems for providing information, we recommend incorporating the controls in these standards from the design stage to operate a compliant cloud service.

■ Related Standards

Aside from ISO 27017, other international standards related to cloud security have been published or are under consideration. Specific examples, including those currently being discussed, are ISO/IEC 17788:2014*[56], 17789:2014*[57], NP 19086-4*[58], 27018:2014*[59], and DIS 27036-4*[60], which we will introduce briefly here. ISO/IEC details are omitted from text below.

17788 contains definitions of what cloud computing is and what types exist, as well as its vocabulary, or in other words cloud computing terms. 17789 describes cloud computing architecture. 27017 is created with these two standards in mind. These two standards are open, and can be freely downloaded from the ISO website and read, so we recommend taking a look. Additionally, 27018 defines guidance for when handling privacy on cloud services. Other standards currently under consideration for standardization include 19086-4, which covers cloud service SLA, and 27036-4, which is approached from a supply chain perspective.

The future use of ISO 27017 as a certification system is also being discussed, and in Japan the Japan Institute for Promotion of Digital Economy and Community (JIPDEC) has indicated they will perform certification*[61]. Once a certification system is established, having cloud services that meet a set security level certified by a third party will make things more transparent, enabling users to evaluate the security provided.

■ Summary

Security is a point of concern when using cloud services, but the international standardization of control measures will create an environment where these services are even easier to use. IIJ’s cloud service, the IIJ GIO Service, is already partially compliant with ISO 27017, and we intend to expand the scope of compliance going forward. IIJ will continue to actively promote the observance of international standards, and offer secure cloud services that provide peace of mind.

1.4.2 The Let’s Encrypt Project and the ACME Protocol for Automatic Certificate Issuing

X.509 certificates*[62] are formatted data that guarantees the relationship between a public key and its owner. They are widely used in secure protocols such as SSL/TLS to securely present server or client public keys. Public key certificates are issued hierarchically within the framework of the PKI (Public Key Infrastructure) system in which the public key stored in the corresponding certificate is trusted by tracing it sequentially from the certificate issuer to the root certificate that serves as a trust anchor*[63]. Server certificates for SSL/TLS sites are sold by commercial CA services*[64], and can be broadly categorized into the three types in Table 1. Of these, DV certificates are only used to confirm whether a party is the domain name owner, so the typical procedure for issuance involves

*56 ISO/IEC 17788:2014 Information technology -- Cloud computing -- Overview and vocabulary (http://www.iso.org/iso/catalogue_detail?csnumber=60544).

*57 ISO/IEC 17789:2014 Information technology -- Cloud computing -- Reference architecture (http://www.iso.org/iso/catalogue_detail?csnumber=60545).

*58 ISO/IEC NP 19086-4 Information technology -- Cloud computing -- Service level agreement (SLA) framework and Technology -- Part 4: Security and privacy (http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=68242).

*59 ISO/IEC 27018:2014 Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors (http://www.iso.org/iso/home/store/catalogue_tc/catalogue_detail.htm?csnumber=61498).

*60 ISO/IEC DIS 27036-4 Information technology -- Security techniques -- Information security for supplier relationships -- Part 4: Guidelines for security of cloud services (http://www.iso.org/iso/catalogue_detail.htm?csnumber=59689).

*61 JIPDEC, “Notice of the start of cloud security certification based on ISMS conformance evaluation system ISO/IEC 27017” (http://www.isms.jipdec.or.jp/topics/ISO27017_CLS.html) (in Japanese).

*62 RFC6818: Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile (https://datatracker.ietf.org/ doc/rfc6818/).

*63 See “1.4.3 Incidents of the Fraudulent Issue of Public Key Certificates” in Vol.13 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol13_EN.pdf) for an explanation of the PKI system.

*64 For example, the following Netcraft site page lists some of the major commercial CA services. Netcraft Ltd., “SSL Survey” (http://www.netcraft.com/internet-data-mining/ssl-survey/).

the domain name owner sending a CSR (Certificate Signing Request) to a CA issuing site, which issues a certificate once the corresponding domain name owner is confirmed. In contrast, OV and EV certificates*65 are for confirming the existence of an organization in the real world, making them significantly different to DV certificates. For this reason, some companies issue DV certificates for free*66, or do not issue them at all. This is thought to be because of a shift to a business model that encourages the purchase of OV or EV certificates instead of DV certificates, to differentiate between them.

The Let's Encrypt project*67 was established with the goal of automatically issuing DV certificates for free. This automatic certificate issuing service is compliant with the ACME (Automated Certificate Management Environment) protocol*68 formulated by the IETF ACME Working Group. In this article, we will give an overview of the Let's Encrypt project, as well as the ACME protocol used in its implementation.

■ Let's Encrypt Project Overview

The Let's Encrypt project provides an automatic issuing service for the server certificates used extensively in SSL/TLS. Until recently it was only accessible to a limited number of test users, but from early December 2015 it became widely available for general use, garnering a lot of attention*69. This activity is run by a non-profit organization called the Internet Security Research Group (ISRG)*70, whose members and sponsors include organizations such as Mozilla, EFF (Electronic Frontier Foundation), Akamai, and Cisco*71. It is also worth noting that major browser vendor Chrome joined as a platinum sponsor in December 2015*72.

The Let's Encrypt project provides reference implementations using the ACME protocol touched upon later. ACME clients (users requesting the issue of a certificate) can use the Let's Encrypt client to communicate with the ACME server (a CA operated by the Let's Encrypt project) and perform processes such as requests for the issue, reissue, or revocation of certificates*73. During the process of these requests, a number of techniques called Domain Validation are provided to confirm whether or not a requestor is the domain name owner. The Let's Encrypt project's explanation of Domain Validation*74 only lists two methods for confirming the domain owner, involving either (1) controlling a DNS record or (2) publishing a Web page on an HTTP server in response to a challenge from the ACME server (CA). However, the implementation also supports (3) SNI (Server Name Indication), which is defined in the ACME protocol. Refer to the latter part of this article for an explanation of each type of Domain Validation.

Table 1: Types of Server Certificate

DV (Domain Validated) Certificates	Certificates are issued after confirming only the existence of the domain name.
OV (Organization Validation) Certificates	Certificates are issued after confirming the location (existence) of an organization.
EV (Extended Validation) Certificates	Certificates are issued following procedures stipulated by the CA/Bowser Forum. Further differentiation from DV/OV certificates is provided, such as changing URLs to green text in browsers.

*65 CA/Browser Forum, "EV SSL Certificate Guidelines" (https://cabforum.org/extended-validation/). Revisions have continued to be made since these were published in 2007.

*66 For example, WoSign (https://buy.wosign.com/free/) and StartCom (https://www.startssl.com/Account).

*67 Let's Encrypt (https://letsencrypt.org/about/).

*68 IETF, "Automated Certificate Management Environment (acme) - Documents" (https://datatracker.ietf.org/wg/acme/documents/).

*69 Let's Encrypt, "Public Beta: December 3, 2015" (https://letsencrypt.org/2015/11/12/public-beta-timing.html).

*70 Internet Security Research Group (ISRG) (https://letsencrypt.org/isrg/). A presentation made by ISRG board member Peter Eckersley (EFF) at Chaos Communication Camp 2015 is available. "Let's Encrypt - A Certificate Authority To Encrypt the Entire Web" (https://media.ccc.de/v/camp2015-6907-let_s_encrypt).

*71 Let's Encrypt, "Current Sponsors" (https://letsencrypt.org/sponsors/).

*72 "Happy to announce that @GoogleChrome is a Platinum sponsor of Let's Encrypt!" (https://twitter.com/letsencrypt/status/679708931984248832).

*73 The "Getting Started" page (https://letsencrypt.org/getting-started/) explains how to install and use the client software (https://github.com/letsencrypt/letsencrypt). "Welcome to the Let's Encrypt client documentation!" (https://letsencrypt.readthedocs.org/en/latest/) contains more detailed information. Information regarding the ACME server reference implementation (https://github.com/letsencrypt/boulder) is also available.

*74 Let's Encrypt, "How It Works" (https://letsencrypt.org/how-it-works/).

A variety of data can be viewed in the current Let's Encrypt project*[75]. This data includes the number of certificates issued, which is reported to be around 700,000 valid certificates that have not been revoked at the time of writing*[76]. According to data regarding the number of issuing requests processed within 24 hours*[77] and the number of successful requests, adding a page to a HTTP server accounts for 70% to 80% of the aforementioned Domain Validation methods, followed by SNI. Meanwhile, the method involving the control of DNS records is currently fluctuating at a few percent. It is also possible to view status and maintenance notifications for each type of server (Web, registration, OCSP servers, etc.) in the Let's Encrypt project*[78].

The certificates issued from the Let's Encrypt project's ACME server are issued from the "Let's Encrypt Authority X1" intermediate CA. At this time, the "Let's Encrypt Authority X1" intermediate CA certificate is a cross root certificate, and has two parents*[79]. One of these, "DST Root CA X3," is stored in the certificate store (trusted root certificate list) of the OSes or FireFox. This means that major browser users can successfully verify server certificates issued from Let's Encrypt without making any changes to the certificate store (without adding a root certificate as a trust anchor). Certificates are set to be valid for 90 days*[80], which is a shorter period of time than server certificates that can be purchased normally. It is explained that this is to reduce the impact when a private key is compromised*[81], or when a certificate is mistakenly issued. Also, because the reissuing process has already been automated in some environments, it is expected that a shorter period of validity won't add to the workload associated with reissuing.

■ ACME Protocol Overview and Development Status

The ACME protocol was discussed after a mailing list was set up in November 2014*[82], and a BOF was held at IETF meeting 92 in March 2015*[83]. In May 2015 they began official activities as the ACME WG*[84], and a gathering was held at the IETF 93 meeting in July*[85]. At this point in time, the draft-barnes-acme-04*[86] was being discussed as the main protocol specification. After draft-barnes-acme was revised between January and July, 2015, acme-acme*[87] appeared as a WG draft based on draft-barnes-acme-04 in September, and at the time of writing the -01 draft had come out. The dates and draft versions have not been properly maintained in the Editor's copy*[88], but these have been added from acme-acme-01, which is the newest version of the specifications. According to the charter, the aim is to present acme-acme to the IESG (Internet Engineering Steering Group)*[89] by March 2016, so discussions regarding the draft still continue at a feverish pace. The details of discussions can be viewed on the GitHub site*[90]. Additionally, acme-acme is currently the only specification treated as a WG draft. The draft-pepanbur-acme-proxy*[91] draft is cited as related, but only acme-acme was discussed at the IETF 94 meeting*[92].

*75 Let's Encrypt Stats (https://letsencrypt.org/stats/).

*76 Daily Activity (https://plot.ly/9/~letsencrypt/).

*77 Challenges (last 24 hours) (https://plot.ly/11/~letsencrypt/).

*78 Let's Encrypt, "All Systems Operational" (https://letsencrypt.status.io/).

*79 The path for certificates in the Let's Encrypt project can be confirmed below. Certificates (https://letsencrypt.org/certificates/). Furthermore, the certificate for letsencrypt.org itself is not issued from the "Let's Encrypt Authority X1" intermediate CA, but from another intermediate CA under IdenTrust.

*80 Why ninety-day lifetimes for certificates? (https://letsencrypt.org/2015/11/09/why-90-days.html). User Guide - Renewal (https://letsencrypt.readthedocs.org/en/latest/using.html#renewal).

*81 Examples of the compromise of cryptographic algorithms are provided in Vol.8 of this report (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol08_EN.pdf) under "1.4.1 Trends in the Year 2010 Issues on Cryptographic Algorithms."

*82 acme@ietf.org Mail Archive (https://www.ietf.org/mailman/listinfo/acme).

*83 ACME (Approved as BOF for IETF 92) (https://trac.tools.ietf.org/bof/trac/wiki/BofIETF92#ACMEApprovedasBOFforIETF92).

*84 Automated Certificate Management Environment (acme): Charter for Working Group (https://datatracker.ietf.org/wg/acme/charter/).

*85 See the ACME WG minutes (https://www.ietf.org/proceedings/93/minutes/minutes-93-acme) or the presentation regarding draft-barnes-acme (https://www.ietf.org/proceedings/93/slides/slides-93-acme-1.pdf) from the IETF 93 meeting.

*86 draft-barnes-acme (https://datatracker.ietf.org/doc/draft-barnes-acme/) (https://letsencrypt.github.io/acme-spec/).

*87 Automatic Certificate Management Environment (ACME) (https://datatracker.ietf.org/doc/draft-ietf-acme-acme/).

*88 Automatic Certificate Management Environment (ACME) Editor's copy (https://ietf-wg-acme.github.io/acme/).

*89 Internet Engineering Steering Group (IESG) (http://www.ietf.org/iesg/).

*90 GitHub, Automatic Certificate Management Environment (ACME) (https://github.com/ietf-wg-acme/acme). The development status with regard to acme-acme is available under Issues (https:// github.com/ietf-wg-acme/acme/issues), and Pull requests (https://github.com/ietf-wg-acme/acme/pulls).

*91 A list of documents handled by the ACME WG can be viewed at the following location, "Automated Certificate Management Environment (acme)" (https://datatracker.ietf.org/wg/acme/documents/). At the time of writing, "ACME Proxy Mode of Operation" (https://datatracker.ietf.org/doc/draft-pepanbur-acme-proxy/) was listed as a related draft.

*92 See the ACME WG log (https://www.ietf.org/proceedings/94/minutes/minutes-94-acme) or the acme-acme presentation materials (https://www.ietf.org/proceedings/94/slides/slides-94-acme-0.pdf) from the IETF 94 meeting.

From here, we will provide an explanation of the ACME protocol based on the Editor's copy of acme-acme-01 (obtained February 12, 2016). ACME is a protocol that passes JSON-formatted[*93] messages for interaction between servers and clients. Basically, an ACME server behaves like an HTTPS server, and ACME messages are protected by HTTPS. The ACME server handles certificate issuing on the CA side, while the ACME clients are the users requesting the issue of certificates. The client software is designed to be run on servers that require server certificates, such as Web servers and email servers. It is stated that both clients and servers should support Public Key Pinning[*94] at this time. Support for Public Key Pinning, in combination with a conventional system that verifies the certificate chain, guarantees that ACME server certificates are legitimate.

All ACME messages sent to servers from clients via HTTPS are signed by the clients using JWS (JSON Web Signature)[*95]. This process enables servers to verify that messages are from the correct client. To provide this system, clients must register their public key to the ACME server before sending certificate issuing requests, etc.[*96]. Specifically, JSON Web Key format[*97] key data is sent to the server along with contact information containing an email address or phone number. When doing this, the public key used for signing is another key called an Account Key Pair, which is used when registering, and differs from the public key used for server certificates. The key used during registration can send certificate issuing requests for a number of FQDN (Fully-Qualified Domain Name). An abstract word "identifier" is used instead of FQDN in these specifications, because future expansion is expected. For this reason, there are no issues with reading "identifier" as "FQDN" at this point in time.

A list of services provided by the ACME server is obtained using a discovery service function called "directory." For example, in the current Let's Encrypt project, clients acquire JSON data by specifying the URL related to the directory[*98].

A number of protocol message types are prescribed in ACME, and clients sign the prescribed data in JWS format and use POST to deliver it to the URL listed in the directory. Here, we will explain by discussing only the basic resources, covering from certificate issue to disposal. Normally, the ACME client carries out a series of processes in the following resource order.

new-reg → new-authz → challenge → new-cert → revoke-cert

After performing registration processing using the new-reg resource, ACME clients sign with the private key from the Account Key pair used at the time of registration. For this reason, ACME servers must manage the Account Key registered by clients. In particular, it is stipulated that a 409 (Conflict) HTTP error be returned when registration is carried out using the same Account Key.

After finishing the registration, the new-authz resource is first used to register the identifier. As mentioned previously, the identifier is the FQDN, so here you would register the FQDN for the server certificate you want to issue. As with new-reg, the ACME client signs in JWS format using the Account Key, enabling the server to recognize that the request is from the owner of the corresponding Account Key. In response to this request, the ACME server returns a list showing which of the Domain

[*93] "RFC7159: The JavaScript Object Notation (JSON) Data Interchange Format" (https://tools.ietf.org/html/rfc7159).

[*94] "RFC7469: Public Key Pinning Extension for HTTP" (https://tools.ietf.org/html/rfc7469). Section 7.2.5 of the IPA's "SSL/TLS Encryption Configuration Guidelines - For a Secure Website (Encryption Configuration Measures)" (https://www.ipa.go.jp/files/000045645.pdf) (in Japanese) describes methods for configuring Public Key Pinning.

[*95] "RFC7515: JSON Web Signature (JWS)" (http://tools.ietf.org/html/rfc7515). URL-safe Base64 encoding methods are also listed in Appendix C. This method involves replacing "+" with "-" and "/" with "_" (underline) after normal Base64 encoding, and deleting "=" padding headers. A similar method is also described in RFC4648. "Base 64 Encoding with URL and Filename Safe Alphabet" (http://tools.ietf.org/html/rfc4648#section-5).

[*96] As of December 2015, new-reg resource messages are apparently not used on Let's Encrypt project's ACME servers, and a new-cert message is sent immediately after obtaining the directory.

[*97] "RFC7517: JSON Web Key (JWK)" (https://tools.ietf.org/html/rfc7517). According to section 4.1, it is possible to describe key data type using the "kty" (Key Type) Parameter, a list of which can be viewed in "RFC7518: JSON Web Algorithms (JWA)" (https://tools.ietf.org/html/rfc7518). RSA was used in the reference implementation of the Let's Encrypt project, but EC is strongly recommended (Recommended+) going forward in RFC7518, and it has been announced that support for ECDSA certificates is provided in the actual Let's Encrypt project (https://twitter.com/letsencrypt/status/697504441075798016).

[*98] Can be obtained from the following URL (https://acme-v01.api.letsencrypt.org/directory). The first item of "new-authz," etc., in the JSON data is called a resource, and in acme-acme-01 five types including directory resources are defined.

Validation methods in Table 2 are possible. The ACME client sends a challenge request using the challenge resource to select one or more methods. After the server confirms the FQDN owner, the results are returned. When successful, preparations for issuing the certificate are complete. The client prepares a public key pair separate to the Account Key (described as a Subject Public Key in the specifications), generates a PKCS#10 Certificate Signing Request (CSR), and in a similar manner provides the JWS format signature with the Account Key, before sending a certificate issuing request using the new-cert resource. The server verifies both the JWS and CSR signatures, issues the certificate, then returns the certificate encoded in DER format. When requesting that a certificate be revoked, the revoke-cert resource is used to send a request housing the corresponding certificate with a JWS format signature.

For Domain Validation, acme-acme-01 stipulates http-01, dns-01, and tls-sni-01 as shown in Table 2. These validation types with an "-01" suffix indicate they are connected with the draft version. Discussion of tls-sni-02 has actually already begun[*99]. Although new type names linked to the draft version will be used when procedures are changed in the future upon the release of new versions of the draft itself, the type names will remain the same if no changes are made to the validation procedures.

Several Points of Concern

The scope for JWS signatures is not rigidly defined, and is at this point worded loosely in the draft. For example, key, authorizations, and certificates fields are defined for the formatting of registration resources, but when a server actually processes new-reg resources, these fields must be ignored. Storing dummy data in hash function input locations that are ignored during processing can be a factor in intermediate CA certificate forgery[*100] and SLOTH attacks[*101] succeeding, so this may leave an opening for potential attack.

Because DV certificates are not for confirming real-world existence, they may be issued to servers intended for malicious purposes. In fact, it was reported in early January 2016 that certificates issued by the Let's Encrypt project were actually used on a Trojan distribution server[*102].

The Let's Encrypt project supports Certificate Transparency (CT)[*103], and because notification of issued certificates is sent to log servers[*104], anyone can view the certificates[*105], so problems related to CT have flared up in Japan since some time ago[*106]. Privacy concerns are one of the points identified. For example, problems with the fact that the FQDN of servers planned for an upcoming

Table 2: Domain Validation Types in acme-acme-01

	Type	Client-Side Processing	Server-Side Processing
HTTP (section 7.2)	http-01	• Generate key-authz data through linking token and account key (public key) • Enable access to http://[FQDN]/.well-known/acme-challenge/[token] on port 80 of the HTTP server, and store key-authz data there	• Generate key-authz data • Access the corresponding URL and verify the correct data is stored there
TLS SNI (section 7.3)	tls-sni-01	• Generate key-authz data • Use the TLS SNI (RFC6066) system to prepare for access via HTTPS • The SNI field at this point is generated from the first 32 and last 32 characters of the hexadecimal form of the SHA 256 digest computed from key-authz • Issue a self-signed certificate with subjectAlternativeName set to the aforementioned SNI field, then set it to the HTTPS server	• Generate key-authz data • Use the TLS SNI system to access the HTTPS server • Verify the subjectAlternativeName in the certificate has been generated correctly
DNS (section 7.5)	dns-01	• Generate key-authz data • After computing the SHA-256 digest of key-authz, generate URL-safe Base64 encoded data • The above data is configured in the DNS TXT record	• Generate key-authz data • Verify it has been generated correctly through a lookup of _acme-challenge.[FQDN]

Each type includes random data called a token in the challenge, and this is a required item. The ACME server uses these tokens to identify challenges, so generating new tokens on the server each time is a requirement. Additionally, because it is necessary to protect against guess attacks, the random data must be generated from at least 128 bits of entropy. Tokens are encoded using an URL-safe Base64 encoding method.

[*99] "Proposed changes to TLS-SNI, autorenewal removal" (https://mailarchive.ietf.org/arch/msg/acme/OnLEcxUa_K30ERLIZl5kAreyyh8).

[*100] "MD5 considered harmful today" (http://www.win.tue.nl/hashclash/rogue-ca/).

[*101] "SLOTH: Security Losses from Obsolete and Truncated Transcript Hashes (CVE-2015-7575)" (https://www.mitls.org/pages/attacks/SLOTH).

[*102] TrendLabs Security Intelligence Blog, "Let's Encrypt Now Being Abused By Malvertisers" (http://blog.trendmicro.com/trendlabs-security-intelligence/lets-encrypt-now-being-abused-by-malvertisers/).

[*103] "Certificate Transparency" (https://www.certificate-transparency.org/). "RFC6962: Certificate Transparency" (https://tools.ietf.org/html/rfc6962).

[*104] "Known Logs" (https://www.certificate-transparency.org/known-logs).

[*105] List of certificates issued by Let's Encrypt Authority X1 (https://letsencrypt.org/certs/lets-encrypt-x1-cross-signed.pem) (https://crt.sh/?Identity=%25&iCAID=7395).

[*106] Kenji Urushima, "Discussion of SSL server certificate public audit records due to Certificate Transparency and resulting issues" (http://www.slideshare.net/kenjiurushima/certificate-transparencyssl) (in Japanese).

service launch can leak before release. In the future, there may be cases in which S/MIME certificates are issued under a similar system that only confirms reachability by email, and CT could cause email addresses to be listed.

At the time of writing there are still points that are unclear, but as mentioned at the start of this report, standardization of the ACME main protocol is moving at a quick pace, and it is possible that identifiers or challenges will be newly expanded upon. Furthermore, from the perspective of implementation and operation, there is also a chance that separate services similar to the Let's Encrypt project will appear. It could be considered that we have reached a turning point in which the current certificate business will evolve.

1.4.3 Guidelines for Dealing with Cyber Attacks and Privacy at Telecommunications Carriers

On November 30, 2015, the Council for Stable Operation of the Internet, which is made up of five communications-related organizations, published the fourth version of the "Guidelines for Dealing with Cyber Attacks and Privacy at Telecommunications Carriers"*[107]. Here we will discuss these guidelines.

■ Background and Overview of Revisions

These guidelines are aimed at providing examples of measures that telecommunications carriers such as ISPs can take to deal with cyber attacks, which change on a daily basis. They are positioned as reference material for telecommunications carriers to implement measures such as the blocking of communications without committing illegal acts, including infringing upon the secrecy of communications, taking into consideration related laws such as the Telecommunication Business Act. Since the first version of these guidelines in 2007, they have been developed and revised by private organizations independently. However, since the third version revised in 2015, Ministry of Internal Affairs and Communications' "Workshop on the Appropriate Way to Handle Cyber Attacks in the Telecommunications Business"*[108] has evaluated the compliance of measures for cyber attacks that cause issues on the private side. Revisions have been carried out to apply these results to the guidelines*[109].

In many cases, the handling of cyber attacks and other issues by telecommunications carriers corresponds to an infringement of secrecy of communication. However, for the purpose of dealing with specific attacks and within the scope of applying limited countermeasure techniques, the illegality of these actions may be rejected as they fall under the category of legitimate business activity. These guidelines indicate the scope of legitimate measures based on the approach summarized by the workshop.

The fourth version revisions have been made based on the workshop's second report*[110], as well as the separately issued "Measures against the unauthorized use of IP phones, etc., by a third party"*[111]. As a result, the title has been changed from the previous "High Volume Communications" to "Cyber Attacks," and measures against the unauthorized utilization of telecommunications services have been added. The following five details regarding countermeasures were also appended.

1. Bolstering of measures against DDoS attacks using DNS functions
2. Alerts to users of home routers or other equipment with vulnerabilities
3. Blocking based on a reputation database related to communications between malware-infected PCs and C&C servers
4. Measures against the misuse of the Internet by exploiting another party's authentication information
5. Measures against the unauthorized use of phone services such as IP phones by exploiting another party's authentication information

*107 Council for Stable Operation of the Internet, "Revisions to the Guidelines for Dealing with Cyber Attacks and Privacy at Telecommunications Carriers" (https://www.jaipa.or.jp/topics/2015/11/post.php) (in Japanese).

*108 Ministry of Internal Affairs and Communications, "Workshop on the Appropriate Way to Handle Cyber Attacks in the Telecommunications Business" (http://www.soumu.go.jp/main_sosiki/kenkyu/denki_cyber/) (in Japanese).

*109 For more information on the "Initial Report of the Workshop on the Appropriate Way to Handle Cyber Attacks in the Telecommunications Business," see Vol.23 of this report under "1.4.3 Workshop on the Appropriate Way to Handle Cyber Attacks in the Telecommunications Business" (http://www.iij.ad.jp/en/company/development/iir/pdf/iir_vol23_EN.pdf).

*110 Ministry of Internal Affairs and Communications, "'Second Report of the Workshop on the Appropriate Way to Handle Cyber Attacks in the Telecommunications Business' and Results of Request for Public Comment Published" (http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000100.html) (in Japanese).

*111 Ministry of Internal Affairs and Communications, "Regarding measures to prevent the unauthorized use of IP phones, etc., by third parties" (http://www.soumu.go.jp/main_content/000367498.pdf) (in Japanese).

Next, we will discuss each of these additions[*112].

■ Bolstering of Measures Against DDoS Attacks Using DNS Functions

In the past few years, DNS amplification attacks have become a major problem. These attacks generate large volumes of traffic using the DNS name resolution function by sending name resolution requests via home routers with access control issues, eliciting responses. Measures for dealing with them were discussed during revisions for the third version of these guidelines. The new revisions indicate approaches and sample countermeasures for attacks[*113] that attempt to overload authoritative servers or cache DNS servers provided by ISPs (p.13 (ki) in the guidelines) by generating large numbers of name resolution requests for nonexistent subdomains. These are also a type of DDoS attack that uses DNS functions. The advice given is to constantly monitor the FQDN of name resolution on the DNS cache server the ISP, etc., provides for user name resolution, then determine and list attack-related FQDN, and block name resolution communications based on that list.

■ Alerts to Users of Home Routers or Other Equipment With Vulnerabilities

Devices such as home routers with configuration or functionality issues are being used as stepping stones in attacks, causing traffic spikes and generating large volumes of communications. This is making DDoS attacks a serious problem for not only DNS, but also other communication protocols such as NTP and SSDP. There are also a growing number of cases in which authentication information is leaked from a device and exploited by third parties. ISPs and industry organizations have conducted field studies regarding the total number of devices like this, but even in cases where it was established a device that connected using a specific IP address has a vulnerability or configuration error, the act of identifying users by referencing contract information related to that IP address constitutes a violation of the secrecy of communications, so it has been withheld to issue alerts or prompt countermeasures. The new revisions cover the legality of this survey activity itself, and state that it is possible to identify users and issue an alert for devices that have vulnerabilities uncovered through the survey results (p.24 (hi) in the guidelines).

■ Blocking Based on a Reputation Database Related to Communications Between Malware-Infected PCs and C&C Servers

In the workshop’s initial report and version 3 of the guidelines, there were discussions about countermeasures that apply access restrictions using URL-related reputation information, and display an alert message, to prevent malware infections that spread via the Web. The principle of consenting to prior contract clauses was also brought up, and it was determined that countermeasures could be implemented as long as an opt-out option is available. The 4th version evaluates measures for infection activity that does not use the Web, as well as those for blocking the communications with C&C servers that occurs after infection due to malware. It is stated that measures implemented by blocking communications at the time of DNS name resolution using an FQDN-related reputation database could be carried out lawfully to achieve this (p.25 (fu) in the guidelines). When using this technique, it is not possible to indicate to users that communications are being blocked or alert them to the presence of malware via Web browser, etc., so it is considered necessary to implement an opt-out policy at the same time by providing a DNS cache server without blocking implemented for users who don’t wish to be affected. Additionally, for the implementation of this, the principle of consent based on contract clauses between the ISP or other organization and the user are examined closely, and at very least the items that should be provided in the clause are indicated (p.14 of the working group’s second report). Furthermore, because this decision on legality is based on the assumption that no users desire to be infected with malware and suffer resulting damages, it was determined that adopting this technique for purposes other than preventing malware infection or activity, such as for preventing access to illegal or harmful content, could constitute a violation of the secrecy of communications (p.12 of the working group’s second report, p.26 (3) in the guidelines).

■ Measures Against the Misuse of the Internet by Exploiting Another Party’s Authentication Information

Due to cases in which the authentication information provided by ISPs for Internet access has been obtained unlawfully from a device such as a home router with a vulnerability, and exploited for crimes by a third party, countermeasures regarding the exploitation of authentication information were discussed. Suggested measures include constantly checking the status of

[*112] In this report we have endeavored to use plain language, to convey the situations looked at in the working group and guidelines in a more easily understandable manner. When actually implementing these measures, it should only be done after examining the written content of the working group’s report and guidelines sufficiently.

[*113] This type of attack is called a Random Subdomain Attack or DNS Water Torture Attack. Secure64 Software Corporation, “Water Torture: A Slow Drip DNS DDoS Attack” (https://blog.secure64.com/?p=377).

authentication on authentication servers at ISPs, etc., and finding authentication attempts that probably indicate unauthorized use. Examples of this would be large numbers of repeated authentication attempts in a short space of time, and cases where movement between regions has taken place so quickly that it wouldn't physically be possible, such as when a user reconnects from Kyushu moments after connecting from Hokkaido. When such unauthorized use is detected, it was indicated that you could shut down authentication processing temporarily based on this information, and contact the user (p.27 (he) in the guidelines).

■ Measures Against the Unauthorized Use of Phone Services Such as IP Phones by Exploiting Another Party's Authentication Information

There have been incidents in which the SIP servers used for IP phones have been accessed without authorization, and international phone calls made illegally, resulting in legitimate users being billed for calls they have no knowledge of*[114]. To deal with this problem, it was indicated that you could periodically monitor the charges to a subscriber's account for international calls, and when these charges spike sharply compared to normal usage, you can analyze the corresponding country, originator's phone number, and source IP address, and determine whether this usage was carried out by a legitimate user. When it seems likely this was not carried out by a legitimate user, measures such as contacting the user, suspending outbound international calls for the corresponding line when the user can't be reached, or temporarily suspending SIP authentication from the corresponding IP address were put forward (p.28 (ho) and p.29 (ma) in the guidelines). Additionally, when measures against unauthorized use such as these fail to have any effect, the technique of temporarily restricting general outgoing traffic for specific countries thought to be misused was also suggested (p.29 (mi) in the guidelines).

■ Summary

As demonstrated here, these guidelines evaluate individual measures for coping with the cyber attacks occurring today, and indicate their legality. When carrying out these measures, the status of attacks at each telecommunications carrier must be taken into account, and a range of criteria such as cost and technical considerations for minimizing secondary effects must be met, so not all of them will be implemented. However, as the situation surrounding cyber attacks changes on a daily basis, it is beneficial for many telecommunications carriers and their users to have guidelines to refer to at a glance should it become necessary.

1.5 Conclusion

This report has provided a summary of security incidents to which IIJ has responded. In this report, we discussed international standards for cloud security, as well as the Let's Encrypt project and the ACME protocol for automatically issuing certificates. We also took a look at the Guidelines for Dealing with Cyber Attacks and Privacy at Telecommunications Carriers. IIJ makes every effort to inform the public about the dangers of Internet usage by identifying and publicizing incidents and associated responses in reports such as this.

Authors:
Mamoru Saito
Manager of the Office of Emergency Response and Clearinghouse for Security Information, Service Operation Division, IIJ. 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 providers Group Japan, and others.

Hirohide Tsuchiya (1.2 Incident Summary)
Hirohide Tsuchiya, Tadaaki Nagao, Hiroshi Suzuki, Hisao Nashiwa (1.3 Incident Survey)
Masahiko Kato (1.4.1 International Standards for Cloud Security)
Yuji Suga (1.4.2 The Let's Encrypt Project and the ACME Protocol for Automatic Certificate Issuing)
Mamoru Saito (1.4.3 Guidelines for Dealing with Cyber Attacks and Privacy at Telecommunications Carriers)
Office of Emergency Response and Clearinghouse for Security Information, Service Operation Division, IIJ

Contributors:
Minoru Kobayashi, Tadashi Kobayashi, Masafumi Negishi, Yasunari Momoi, Hiroyuki Hiramatsu, Office of Emergency Response and Clearinghouse for Security Information, Service Operation Division, IIJ

*[114] Ministry of Internal Affairs and Communications, "Regarding measures to prevent the unauthorized use of IP phones, etc., by third parties (request)" (http://www.soumu.go.jp/menu_news/s-news/01ryutsu03_02000096.html) (in Japanese).