JPCERT-IR-2018-01

Issued: 2018-01-16

JPCERT/CC Incident Handling Report
[October 1, 2017 – December 31, 2017]

1. About the Incident Handling Report

JPCERT Coordination Center (herein, JPCERT/CC) receives reports on computer security incidents (herein, incidents) that occur inside and outside Japan(*1). This report will introduce statistics and case examples for incident reports received during the period from October 1, 2017 through December 31, 2017.

[*1] A "Computer Security Incident", for the purpose of this report, refers to all events that may occur in the management of information systems, which include events that may be considered security issues and any case related to computer security.

JPCERT/CC's activities are aimed at recognition and handling of incidents for Internet users and to prevent the spreading of damages from incidents. For incidents that require global coordination and assistance, JPCERT/CC acts as the point of contact for Japan and performs coordination with relevant parties domestically and globally (overseas CSIRTs, etc.).

2. Quarterly Statistics

[Chart 1] shows the total number of incident reports, reported incidents and incidents that JPCERT/CC coordinated during this quarter.

[Chart 1 Number of incident reports]

	Oct	Nov	Dec	Total	Last Qtr. Total
Number of Reports *2	1460	1596	1474	4530	4600
Number of Incident *3	1522	1710	1503	4735	4811
Cases Coordinated *4	621	576	704	1901	2234

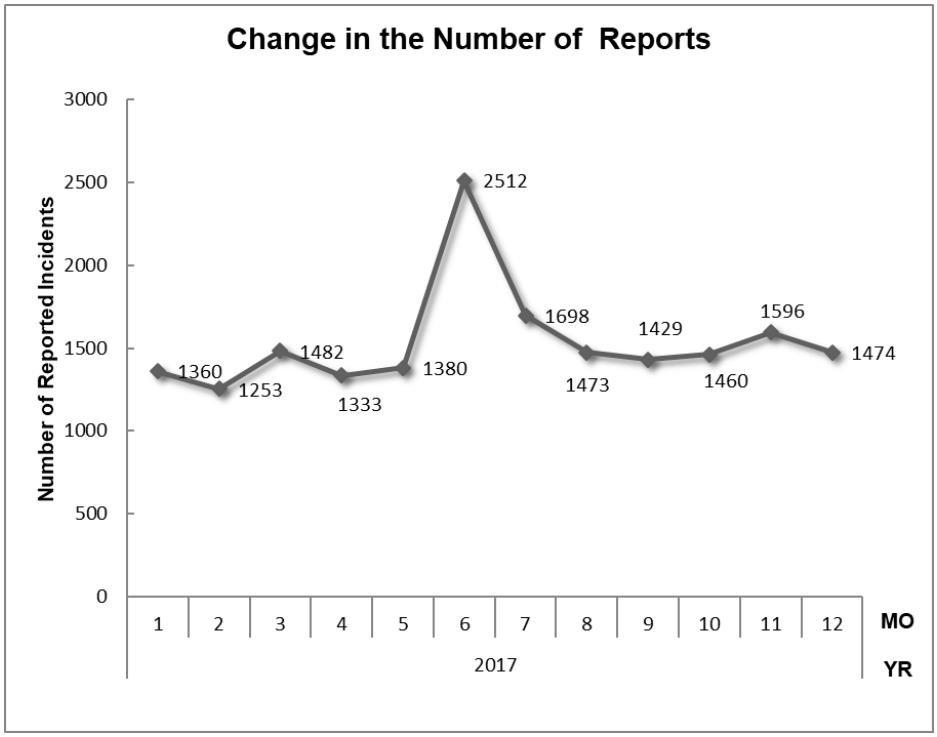
[*2] "Number of Reports" refers to the total number of reports sent through the web form, e-mail or FAX.

[*3] "Number of Incidents" refers to the number of incidents contained in each report.
Multiple reports on the same incident are counted as 1 incident.

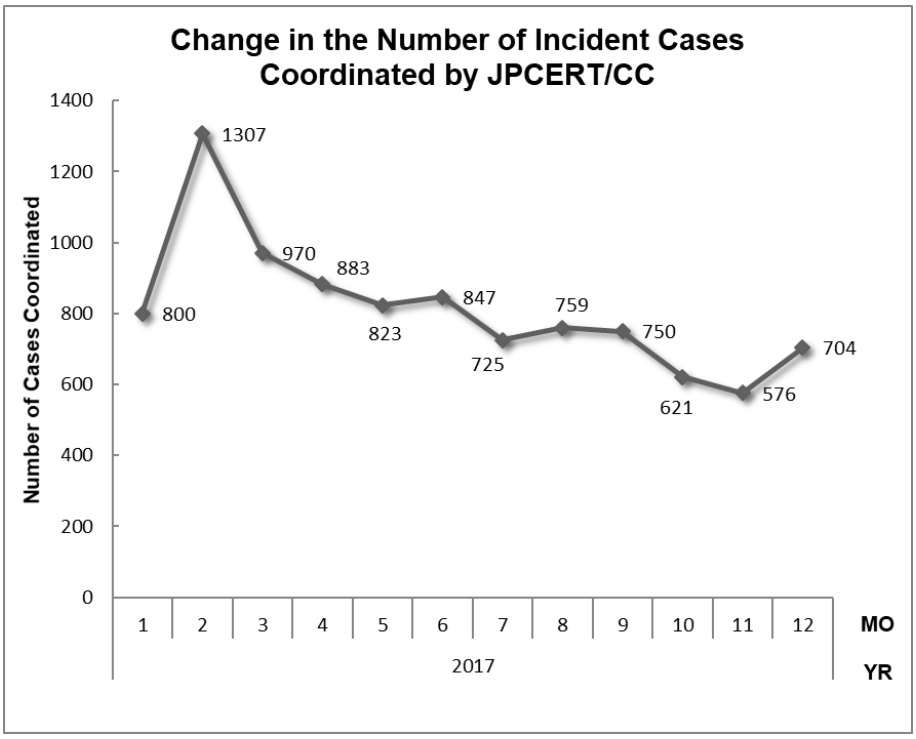
[*4] "Number of Cases Coordinated" refers to the number of cases where coordination took place to prevent the spreading of an incident by sending them a report and asking the site administrator to address any issues.

The total number of reports received in this quarter was 4,530. Of these, the number of domestic and overseas sites that JPCERT/CC coordinated with was 1,901. When compared with the previous quarter, the total number of reports decreased by 2%, and the number of cases coordinated decreased by 15%. Year on year, the number of reports increased by 12%, and the number of cases coordinated decreased 34%.

[Figure 1] and [Figure 2] show the monthly changes in the total number of reports and incident cases coordinated by JPCERT/CC over the past fiscal year.



[Figure 1 Change in the number of incident reports]



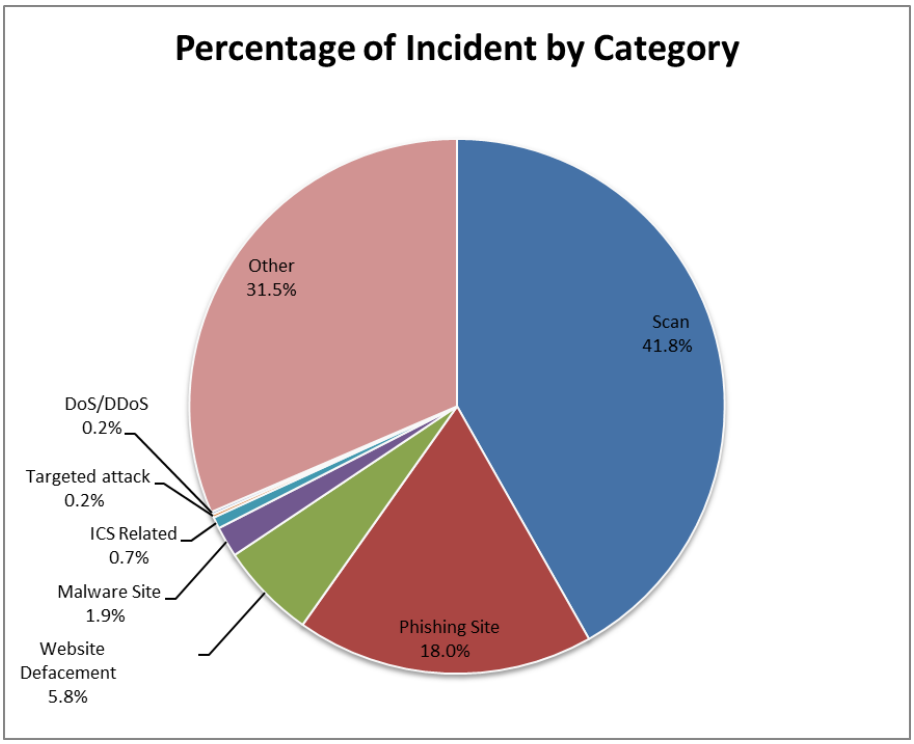
[Figure 2 Change in the number of incident cases coordinated]

At JPCERT/CC, incident reports that were received are categorized, coordinated and handled according to the incident category that they fall into. For definitions on each incident category, please see "Appendix 1 - Incident Categories." [Chart 2] shows the number of incidents received per category in this quarter.

[Chart 2: Number of incidents by category]

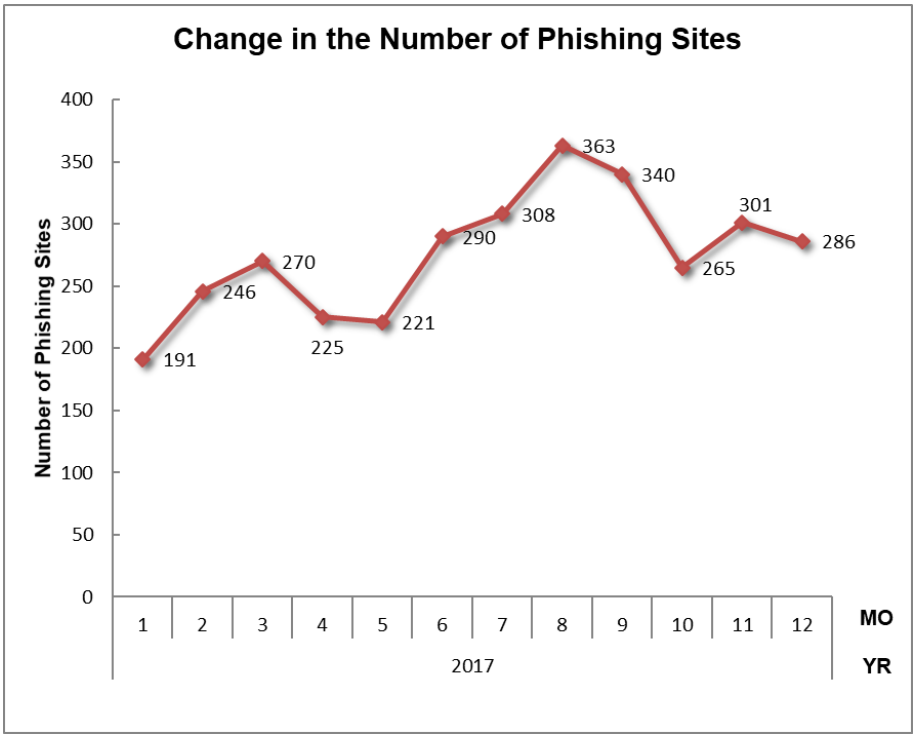
Incident Category	Oct	Nov	Dec	Total	Last Qtr. Total
Phishing Site	265	301	286	852	1011
Website Defacement	111	69	96	276	254
Malware Site	26	28	34	88	98
Scan	668	687	624	1979	2554
DoS/DDoS	6	2	0	8	7
ICS Related	9	12	12	33	13
Targeted attack	5	4	0	9	7
Other	432	607	451	1490	867

The percentage that each category represents over the total number of incidents in this quarter is shown in [Figure 3]. Incidents categorized as scans, which search for vulnerabilities in systems, accounted for 41.8%, and incidents categorized as phishing sites made up 18.0%.

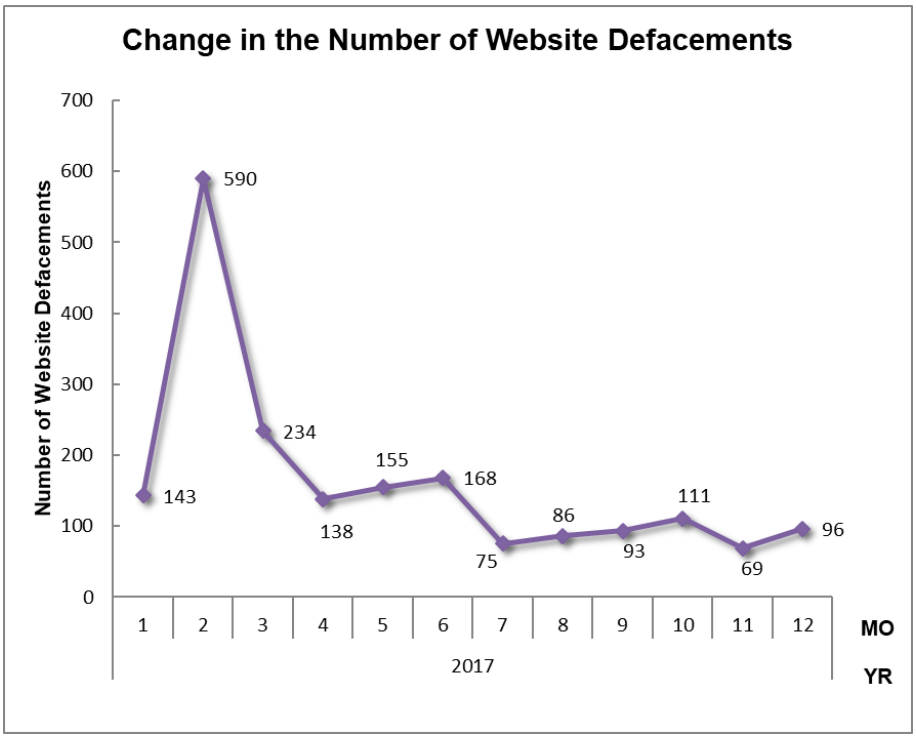


[Figure 3 Percentage of incidents by category]

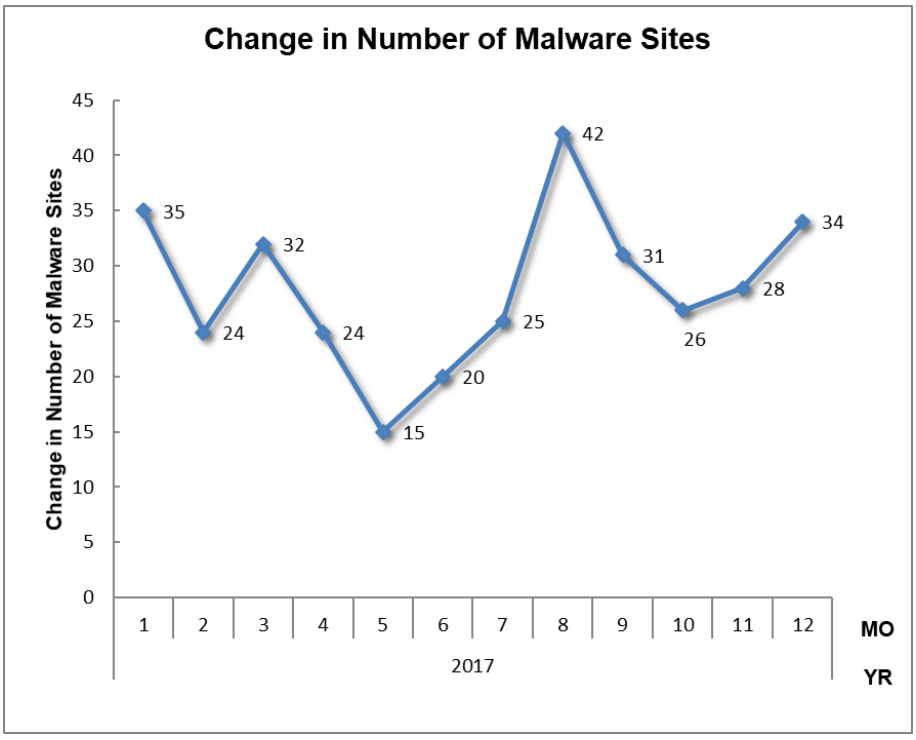
[Figure 4] through [Figure 7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



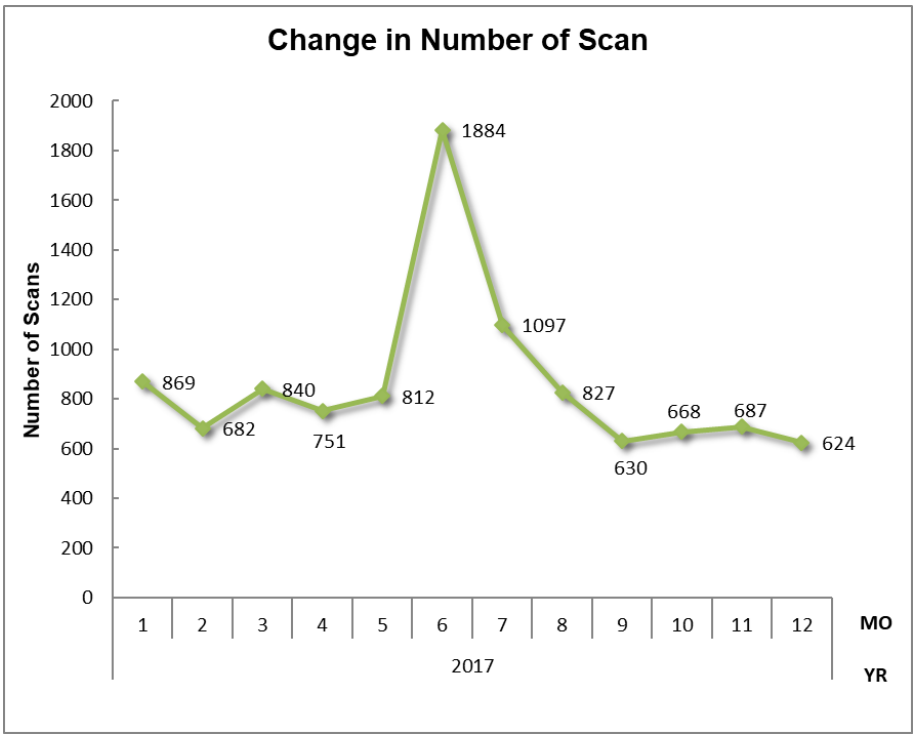
[Figure 4 Change in the number of phishing sites]



[Figure 5 Change in the number of website defacements]

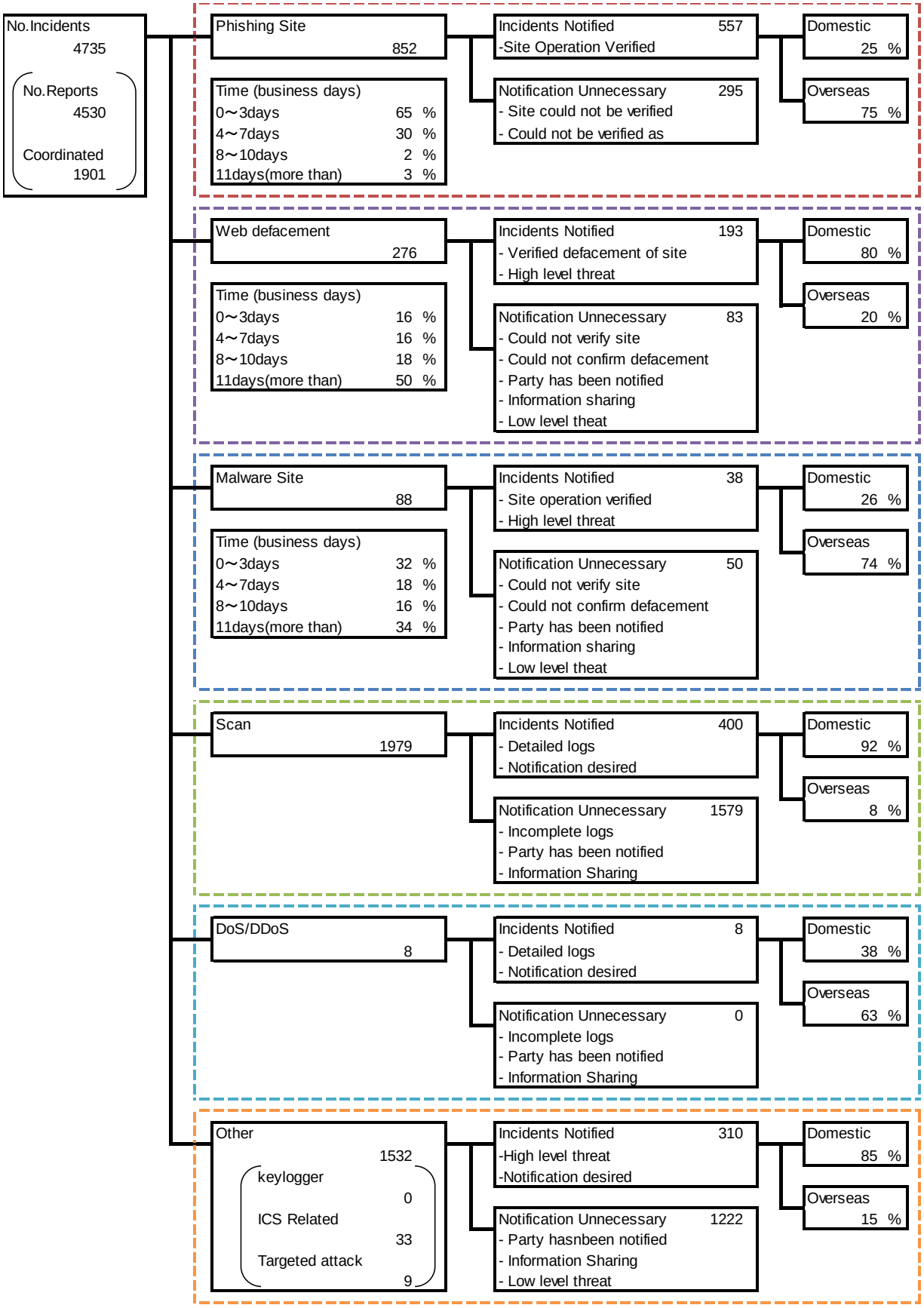


[Figure 6 Change in the number of malware sites]



[Figure 7 Change in the number of scans]

[Figure 8] provides an overview as well as a breakdown of the incidents that were coordinated / handled.



[Figure 8 Breakdown of incidents coordinated/handled]

3. Incident Trends

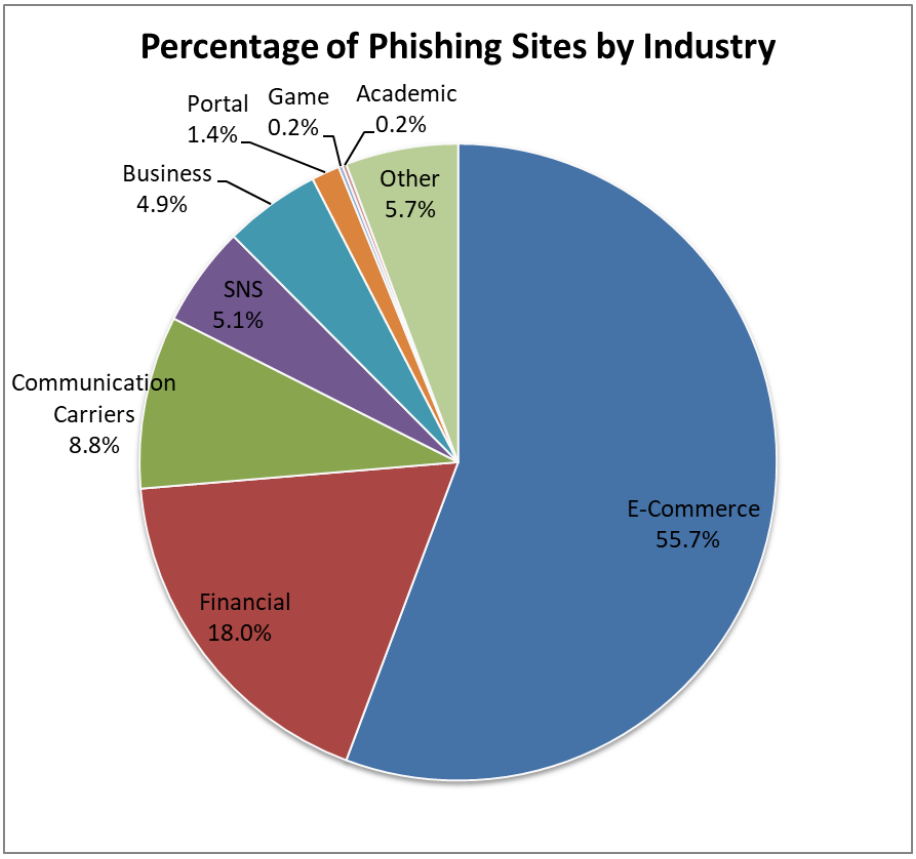
3.1. Phishing Site Trends

During this quarter, 852 reports on phishing sites were received, representing a 16% decrease from 1,011 in the previous quarter. This marks a 64% increase from the same quarter last year (521). The breakdown of the brand type (domestic, overseas) that the phishing sites spoofed in this quarter is shown in [Chart 3], and a breakdown by industry is shown in [Figure 9].

[Chart 3 Number of reported phishing sites by domestic/overseas brand]

Phishing Site	Oct	Nov	Dec	Domestic/ Overseas Total (%)
Domestic Brand	42	32	43	117(14%)
Overseas Brand	192	216	191	599(70%)
Unknown Brand [*5]	31	53	52	136(16%)
Monthly Total	265	301	286	852(100%)

[*5] "Unknown Brand" refers to sites which could not be verified since the reported site had already been suspended when accessed for confirmation.



[Figure 9 Percentage of reported phishing sites by industry]

During this quarter, there were 117 phishing sites that spoofed domestic brands, decreasing 32% from 173 in the previous quarter. There were 599 phishing sites that spoofed overseas brands, decreasing 13% from 686 in the previous quarter.

Out of the total number of phishing site reports that JPCERT/CC received, 55.7% spoofed e-commerce websites, 18.0% websites of financial institutions, and 8.8% websites of telecommunications carriers.

While 70% of the brands that the phishing sites spoofed were overseas brands, 14% were domestic brands. The greater proportion of overseas brands is attributable to the high number of reports received on phishing e-mails spoofing specific overseas brands. JPCERT/CC investigated some of the websites that are accessed from these phishing e-mails and found that the websites function as phishing sites only when the browser's language is set to Japanese. With other languages, the websites show a message that says the website is suspended. These phishing sites apparently target only Japanese users.

As for phishing sites spoofing domestic brands, there were many reports regarding phishing sites spoofing the web-based e-mail services of telecommunications carriers and .cn domain phishing sites spoofing an SNS. JPCERT/CC has identified that free overseas services that allow users to easily set up a website are often used to create phishing sites designed to steal personal information by spoofing the web-based e-mail services of domestic telecommunications carrier brands and Japanese universities.

The parties that JPCERT/CC contacted for coordination of phishing sites were 25% domestic and 75% overseas for this quarter, indicating an increase in the proportion of domestic parties compared to the previous quarter (domestic: 24%, overseas: 76%).

3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 276. This was a 9% increase from 254 in the previous quarter.

JPCERT/CC has confirmed numerous cases in which a script planted in a website redirects visitors to a fraudulent website that displays a message warning of a malware infection, urging them to call a fake support center, or a website that urges the visitors to download a suspicious tool. There are also cases in which visitors are redirected to a fraudulent support website from a blog page, or from domain parking that displays an ad when an unused domain has been accessed. Users are redirected to fraudulent websites by means of a script or the transfer settings of a page that is brought up from a legitimate blog component or an ad, and there is a possibility that ad delivery networks are being exploited.

Since early October, JPCERT/CC has been receiving reports on websites embedded with a script that runs a process (mining) related to virtual currency on the visitor's device. While some of these websites appear to have been altered and embedded with such a script, others were apparently using a script intentionally written by the website administrator.

3.3.Targeted Attack Trends

There were 9 incidents categorized as a targeted attack. This was a 29% increase from 7 in the previous quarter. JPCERT/CC asked 7 organizations to take action this quarter.

From the end of October to early November, JPCERT/CC confirmed incidents of e-mail spoofing that appeared to be a targeted attack. In these cases, the e-mails had an attachment that exploits the Dynamic Data Exchange (DDE) protocol of Microsoft Office documents. A spoofed e-mail reported at the end of October had a DOCX attachment embedded with DDE fields. When this document file is opened, a dialog is displayed asking whether to launch an application. If the application is launched, communication is established with a C&C server. In another case reported in early November, an MSG file designed to exploit DDE was attached to a spoofed e-mail. When this file is opened, a dialog is displayed asking for input. A response indicating permission will download an HTTP bot from a C&C server and run it. This enables the attacker to execute any function on the device infected with the HTTP bot. Similar methods of attack exploiting DDE to cause malware infection have also been confirmed in incidents that are not targeted attacks. In early November, Microsoft released a security advisory(*1) entitled, "Securely opening Microsoft Office documents that contain Dynamic Data Exchange (DDE) fields."

JPCERT/CC continued to observe the attack method of causing malware infection by getting e-mail recipients to open a shortcut file (LNK file) contained in an attachment, a method that was seen in the previous quarter. In a case reported in late October, an LNK file was contained in a ZIP file attached to a spoofed e-mail. JPCERT/CC confirmed that when the LNK file is opened, a PowerShell script is downloaded and executed, resulting in infection with PlugX, a remote access trojan.

In another case of e-mail spoofing reported in mid-November, an attacker obtained information about a legitimate e-mail that the target organization received and used that information to send the target organization an e-mail that was made to look like a resend and contained a link to download a file used to carry out an attack. Clicking the link downloads a ZIP file containing an LNK file that runs a PowerShell script. When opened, the LNK file installs malware that allows an attacker to remotely upload and download files or execute commands.

3.4. Other Incident Trends

The number of malware sites reported in this quarter was 88. This was a 10% decrease from 98 in the previous quarter. Since around mid-October, JPCERT/CC has been continually observing cases of malware infection intended to steal information and caused by opening a file downloaded from a link contained in a fake e-mail spoofing a financial institution or a credit card company. Numerous related reports were also received.

The number of scans reported in this quarter was 1,979. This was a 23% decrease from 2,554 in the previous quarter. The ports that the scans targeted are listed in [Chart 4].

[Chart 4: Number of scans by port]

Port	Oct	Nov	Dec	Total
22/tcp	457	458	333	1248
25/tcp	91	101	109	301
80/tcp	32	54	30	116
23/tcp	12	19	54	85
21/tcp	9	10	26	45
2323/tcp	1	6	24	31
445/tcp	7	2	16	25
443/tcp	3	4	11	18
3389/tcp	6	2	5	13
53/udp	9	0	1	10
2222/tcp	7	0	1	8
9000/tcp	5	1	1	7
4752/udp	1	2	3	6
110/tcp	2	3	1	6
81/tcp	2	1	1	4
52869/tcp	0	0	4	4
143/tcp	1	1	2	4
123/udp	0	4	0	4
26551/udp	3	0	0	3
1433/tcp	1	1	1	3
Unknown	580	298	581	1459
Monthly Total	1229	967	1204	3400

Ports targeted frequently were SSH (22/TCP), SMTP (25/TCP) and HTTP (80/TCP).

There were 1,490 incidents categorized as other. This was a 72% increase from 867 in the previous quarter.

4. Incident Handling Case Examples

This section will describe some actual cases that JPCERT/CC handled in this quarter.

(1) Coordination involving DNS servers in Japan that allows resource records to be updated from outside
Around mid-October, overseas security researchers provided information about vulnerable DNS servers in Japan that were configured to allow resource records to be updated from outside, along with information about domains that were affected by those servers. The DNS servers were configured to allow dynamic update without any access control or authentication for the updater. As such, it was possible to register any subdomain or edit the IP address of an existing domain, and the servers could potentially be exploited to lure Internet users to a malicious website or steal information. Measures to prevent such exploitation include disabling dynamic update and enabling TSIG, which makes it possible to perform authentication by signing DNS messages.

Based on the provided information, JPCERT/CC contacted the organizations that administer the DNS servers and asked them to review the DNS settings and provide information about the environment in which they use their DNS servers. Some of the organizations contacted explained that dynamic update had been enabled unintentionally, or that they were actually using dynamic update but had not taken appropriate security measures.

(2) Coordination in response to an increase in scans targeting 23/TCP and 2323/TCP
Since early November, TSUBAME, an Internet threat monitoring system operated by JPCERT/CC, has been observing an increase in scans targeting ports 23/TCP and 2323/TCP by packets sent from IP addresses in Japan. Domestic telecommunications carriers and security organizations have also provided similar information regarding such scan activities. At around the same time, a rise was also observed in the number of scans targeting port 52869/TCP at IP addresses in Japan.

As a result of investigations, it was found that router products that were infected with malware due to a scan targeting port 52869/TCP were carrying out scans in order to spread infection. The malware that the router products were infected with was a malware variant called Mirai, which is capable of sending communications using various protocols to any target according to external commands, and which forms

a botnet that was used to carry out a massive DDoS attack. Infected devices may be used as a springboard to launch a DDoS attack if appropriate steps are not taken.

On December 19, JPCERT/CC released “Alert Regarding Mirai Variant Infections”(*2) in cooperation with Japanese organizations that were investigating and otherwise responding to this matter.

5. References

(1) Microsoft Security Advisory 4053440
https://technet.microsoft.com/en-us/library/security/4053440.aspx

(2) Alert Regarding Mirai Variant Infections
https://www.jpcert.or.jp/english/at/2017/at170049.html

Request from JPCERT/CC

JPCERT/CC is working to prevent the spread of losses and damages due to incidents and their recurrence through various activities. These include understanding the status and tendency of incidents, and coordination with the aim of suspending or blocking, as the situation requires, attack sources and destination of information transmission, etc. JPCERT/CC also issues alerts and other information to users to make them aware of the need to implement countermeasures.

JPCERT/CC asks for your continued cooperation with information sharing. Please refer to the following web pages for how to report incidents.

Reporting an Incident
https://www.jpcert.or.jp/english/ir/form.html

Reporting an ICS Incident
https://www.jpcert.or.jp/english/cs/how_to_report_an_ics_incident.html

If you would like to encrypt your report, please use JPCERT/CC's PGP public key. The public key can be obtained at the following web page.

PGP Public Key
https://www.jpcert.or.jp/english/ir/pgp.html

JPCERT/CC provides a mailing list to ensure speedy delivery of the information it issues. If you wish to use the mailing list, please refer to the following information.

Appendix-1 Classification of Incidents

JPCERT/CC classifies incidents contained in reports it receives according to the following definitions.

○ Phishing Site

A "phishing site" refers to a site that spoofs the legitimate site of a bank, auction or other service operators to carry out "phishing fraud" intended to steal user information including IDs, passwords and credit card numbers.

JPCERT/CC classifies the following as "phishing sites".

- Websites made to resemble the site of a financial institution, credit card company, etc.
- Websites set up to guide visitors to a phishing site

○ Website Defacement

"Website defacement" refers to a site whose content has been rewritten by an attacker or malware (including the embedding of a script unintended by the administrator).

JPCERT/CC classifies the following as "website defacement".

- Sites embedded with a malicious script, iframe, etc., by an attacker, malware, etc.
- Sites whose information has been altered by an SQL injection attack

○ Malware Site

A "malware site" refers to a site that infects the computer used to access the site with malware, or a site on which malware used for attack is made publicly available.

JPCERT/CC classifies the following as "malware sites".

- Sites that attempt to infect the visitor's computer with malware
- Sites on which an attacker makes malware publicly available

○ Scan

A "scan" refers to an access made by an attacker (that does not affect the system) to check for the existence of computers, servers and other systems targeted for attack, or to search for vulnerabilities (security holes, etc.) that can be exploited to make unauthorized intrusion into systems. It also includes attempts to infect by malware, etc.

JPCERT/CC classifies the following as "scans".

- Vulnerability searches (checking the program version, service operation status, etc.)
- Attempts to make an intrusion (those that failed)
- Attempts to infect by malware (viruses, bots, worms, etc.) (those that failed)
- Brute force attacks targeting ssh, ftp, telnet, etc. (those that failed)

○ DoS/DDoS

"DoS/DDoS" refers to an attack against servers and/or computers on a network, and network resources including devices and connection lines that make up a network, with an attempt to make a service unavailable.

JPCERT/CC classifies the following as "DoS/DDoS".

- Attacks that exhaust network resources with a large volume of traffic, etc.
- Reduction or suspension of server program responses due to a large access volume
- Service interference by sending a large volume of e-mail (error e-mail, SPAM e-mail, etc.)

○ ICS Related Incident

An "ICS related incident" refers to an incident related to ICS or plants.

JPCERT/CC classifies the following as an "ICS related incident".

- ICSs that are subject to attack via the Internet
- Servers that malware targeting ICSs communicates with
- Attacks that cause abnormal operations of an ICS

○ Targeted attack

A "targeted attack" is a type of attack in which specific organizations, companies, or industries are targeted for malware infection or unauthorized access.

JPCERT/CC categorizes the following as a targeted attack.

- Spoofed e-mail with malware attached sent to a specific organization
- Defacement of a website affected to limited organizations
- A fake website accessible to limited organizations and attempting to infect site visitor's computer
- A command and control server that specially crafted malware communicates with

○ Other

"Other" refers to incidents other than the above.

The following are examples of incidents that JPCERT/CC classifies as "other".

- Unauthorized intrusion into a system exploiting a vulnerability, etc.
- Unauthorized intrusion by a successful brute force attack targeting ssh, ftp, telnet, etc.
- Stealing of information by malware with a keylogger function
- Infection by malware (viruses, bots, worms, etc.)

These activities are sponsored by the Ministry of Economy, Trade and Industry as part of the "Coordination Activities for International Cooperation in Responding to Cyber Attacks for the 2017 Fiscal Year".