JPCERT-IR-2018-01

Issued: 2018-04-12

JPCERT/CC Incident Handling Report
[January 1, 2018 - March 31, 2018]

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 January 1, 2018 through March 31, 2018.

[*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]

	Jan	Feb	Mar	Total	Last Qtr. Total
Number of Reports *2	1,339	1,170	1,277	3,786	4,530
Number of Incident *3	1,424	1,223	1,210	3,857	4,735
Cases Coordinated *4	807	684	712	2,203	1,901

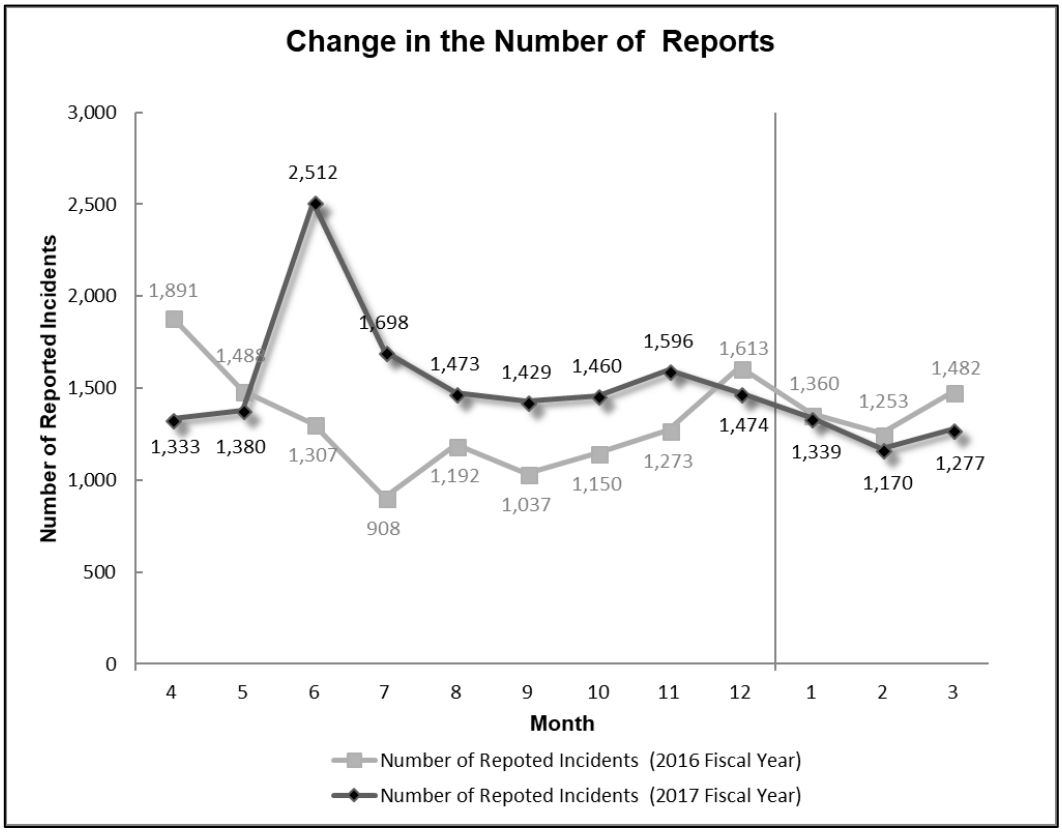
[*2] "Number of Reports" refers to the total number of reports sent through the web form, e-mail or FAX.

[*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.

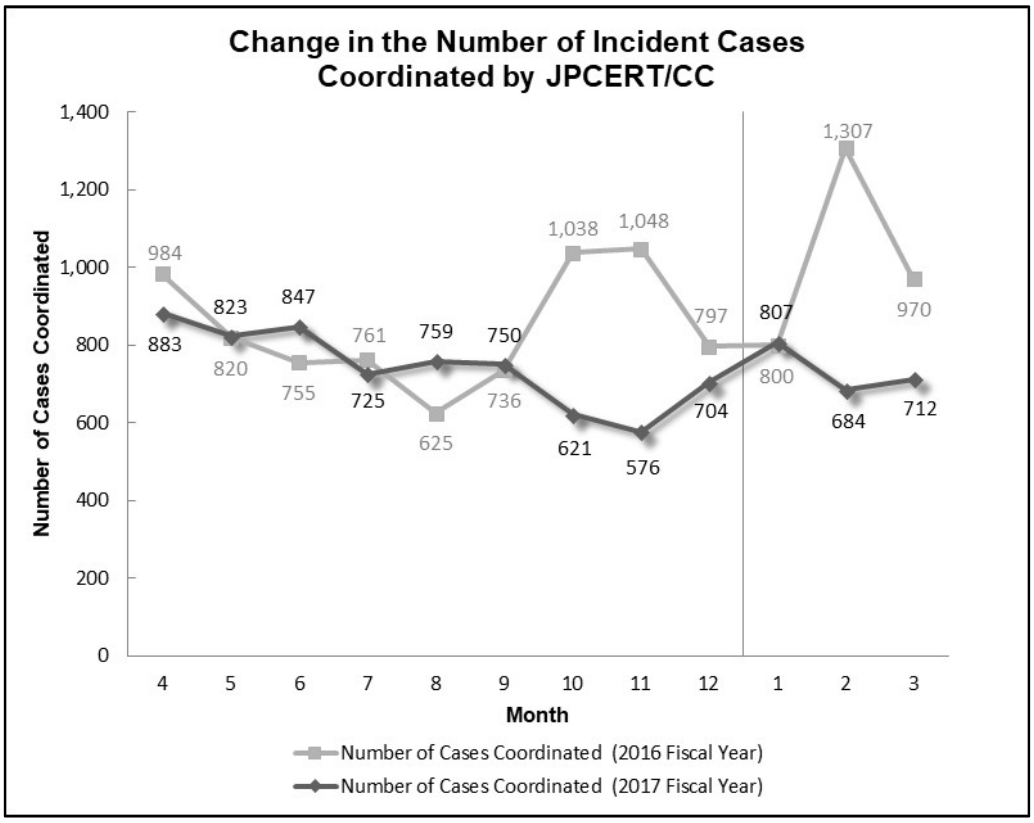
[*4] "Number of Cases Coordinated" refers to the number of cases where coordination took place to prevent the spreading of an incident by sending them a report and asking the site administrator to address any issues.

The total number of reports received in this quarter was 3,786. Of these, the number of domestic and overseas sites that JPCERT/CC coordinated with was 2,203. When compared with the previous quarter, the number of reports decreased by 16%, and the number of cases coordinated increased by 16%. When compared with the same quarter of the previous year, the total number of reports decreased by 8%, and the number of cases coordinated decreased by 28%.

[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]

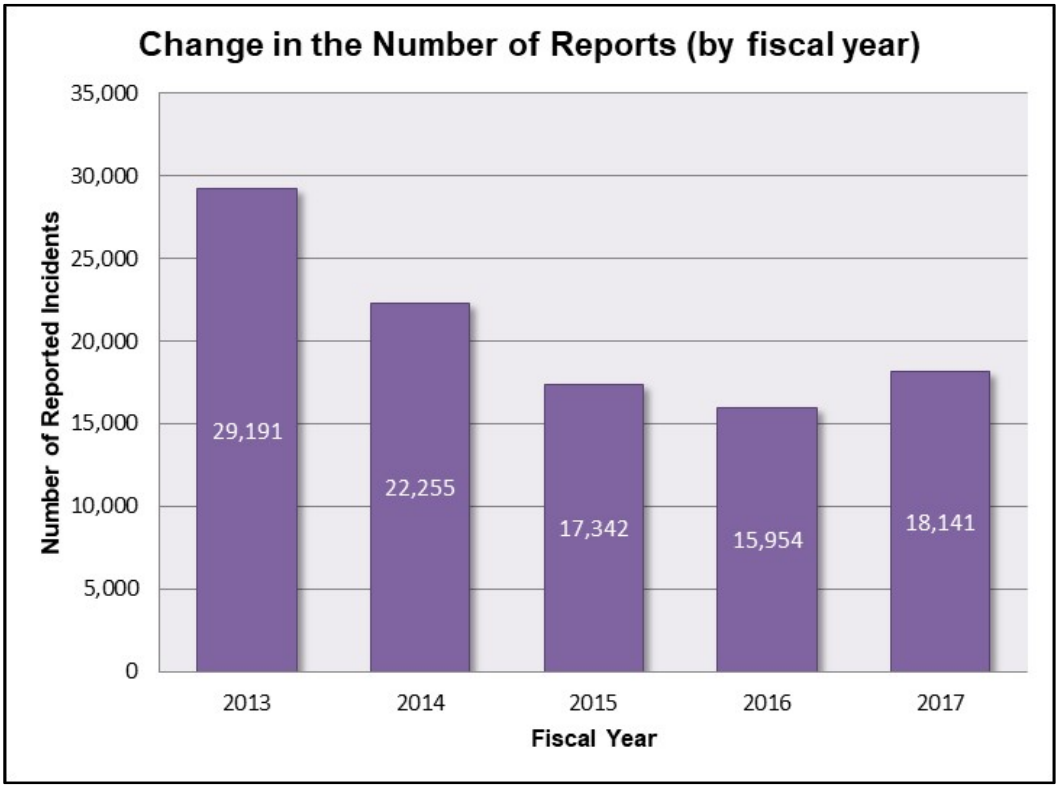
[Reference] Statistical Information by Fiscal Year

[Chart 2] shows the number of reports in each fiscal year over the past 5 years including FY2017. Each fiscal year begins on April 1 and ends on March 31 of the following year.

[Chart 2: Change in the total number of reports]

FY	2013	2014	2015	2016	2017
Number of Reports	29,191	22,255	17,342	15,954	18,141

The total number of reports received in FY2017 was 18,141. This marked a 14% increase from the 15,954 reports received in the previous fiscal year. [Figure 3] shows the change in the total number of reports in the past 5 years.



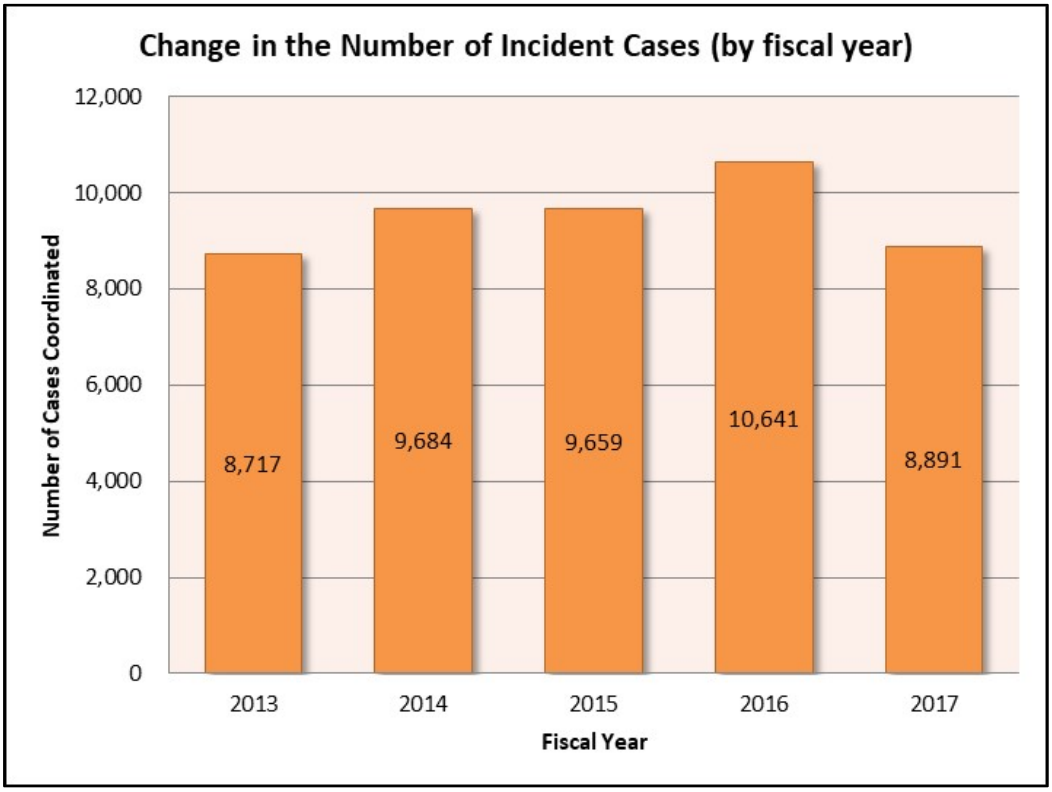
[Figure 3: Change in the total number of reports (by fiscal year)]

[Chart 3] shows the number of cases coordinated in each fiscal year over the past 5 years including FY2017.

[Chart 3: Change in the number of reports and cases coordinated]

FY	2013	2014	2015	2016	2017
Number of Cases Coordinated	8,717	9,684	9,659	10,641	8,891

The total number of cases coordinated in FY2017 was 8,891. This marked a 16% decrease from the 10,641 reports received in the previous fiscal year. [Figure 4] shows the change in the total number of cases coordinated in the past 5 years.



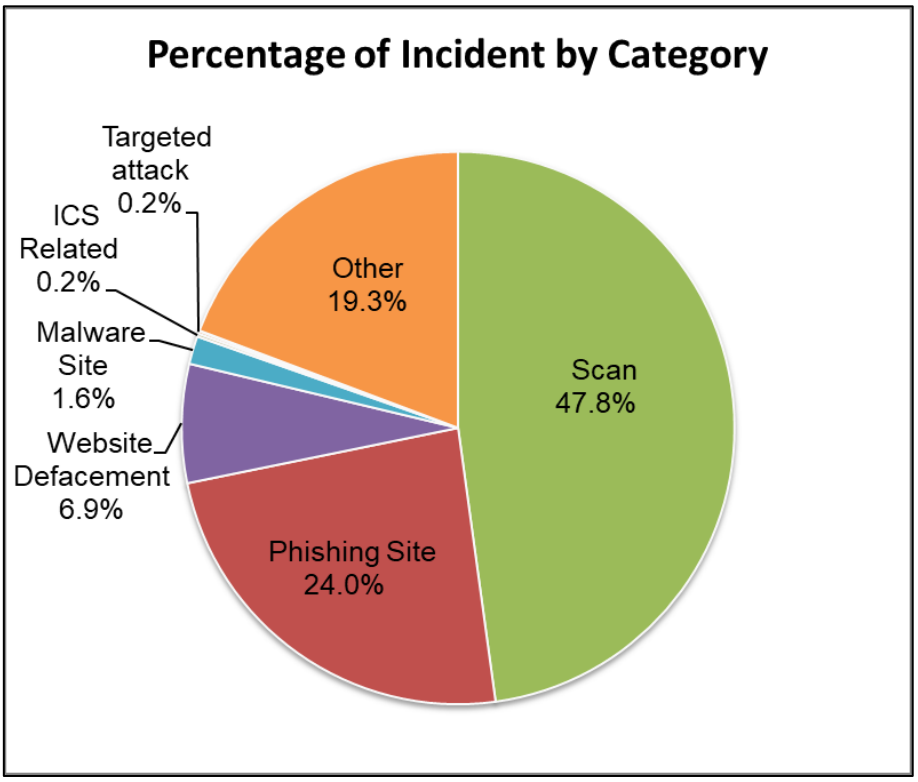
[Figure 4: Change in the Number of Incident Cases (by fiscal year)]

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 4] shows the number of incidents reported per category in this quarter.

[Chart 4: Number of incidents by category]

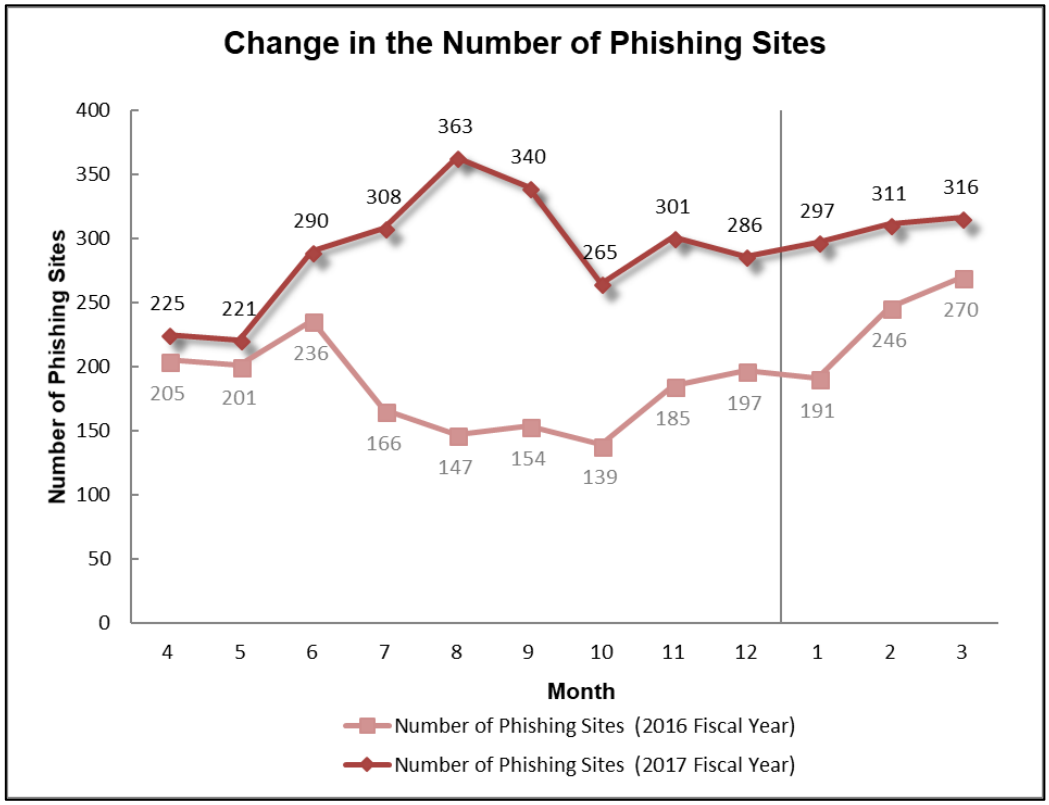
Incident Category	Jan	Feb	Mar	Total	Last Qtr. Total
Phishing Site	297	311	316	924	852
Website Defacement	122	77	69	268	276
Malware Site	24	17	22	63	88
Scan	684	618	543	1,845	1,979
DoS/DDoS	0	1	0	1	8
ICS Related	2	0	5	7	33
Targeted attack	2	2	2	6	9
Other	293	197	253	743	1,490

The percentage that each category represents over the total number of incidents in this quarter is shown in [Figure 5]. Incidents categorized as scans, which search for vulnerabilities in systems, accounted for 47.8%, and incidents categorized as phishing sites made up 24.0%.

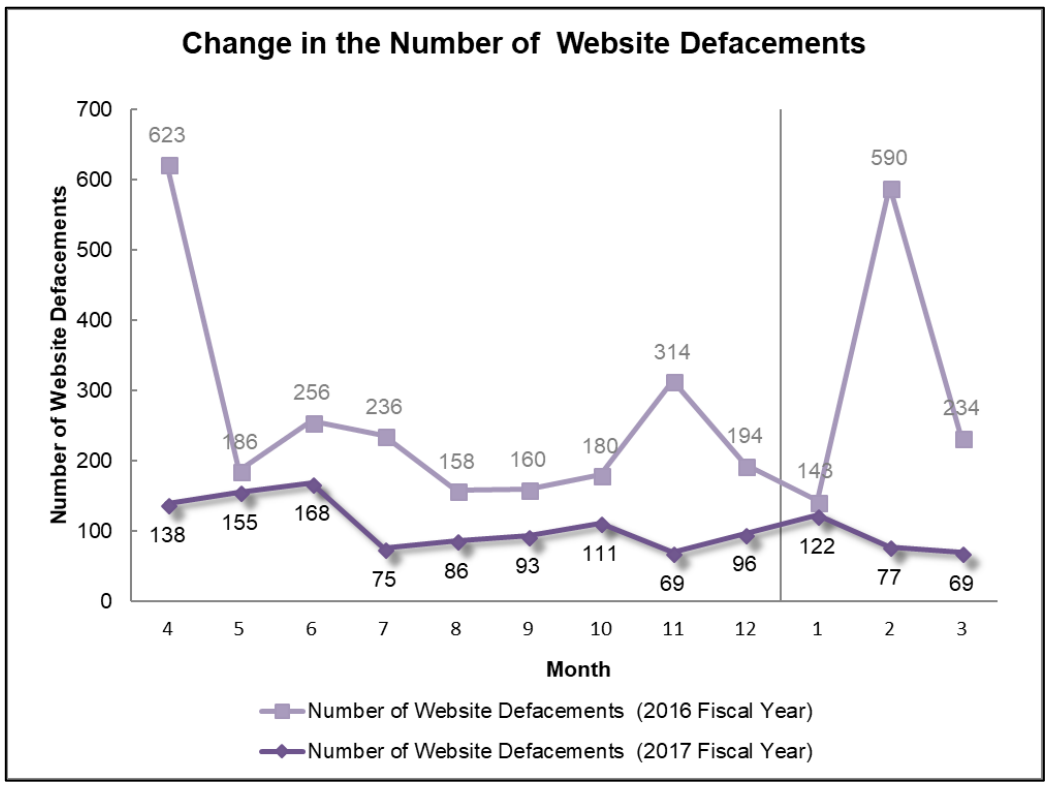


[Figure 5: Percentage of incidents by category]

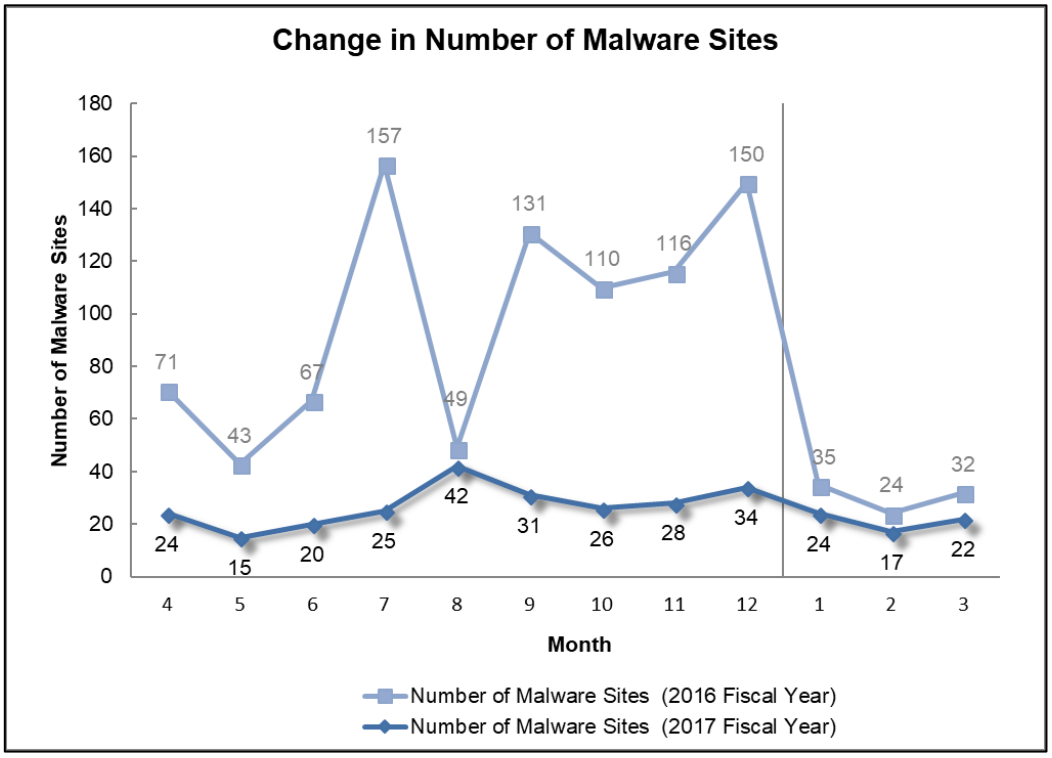
[Figure 6] through [Figure 9] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



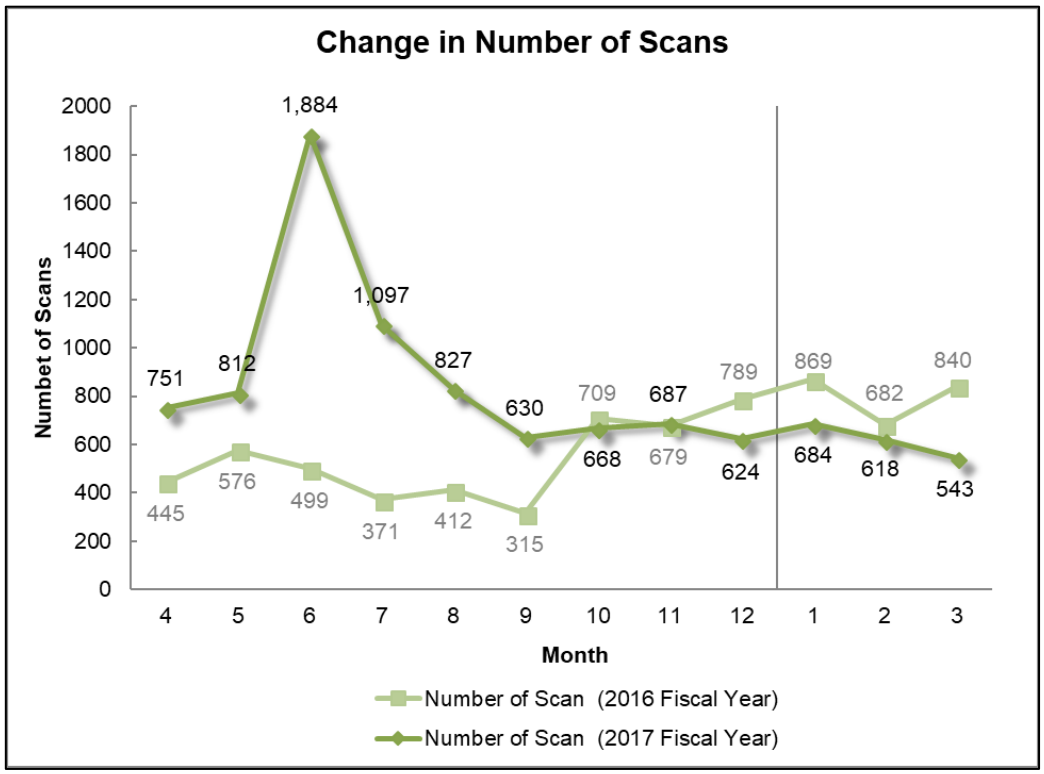
[Figure 6: Change in the number of phishing sites]



[Figure 7: Change in the number of website defacements]

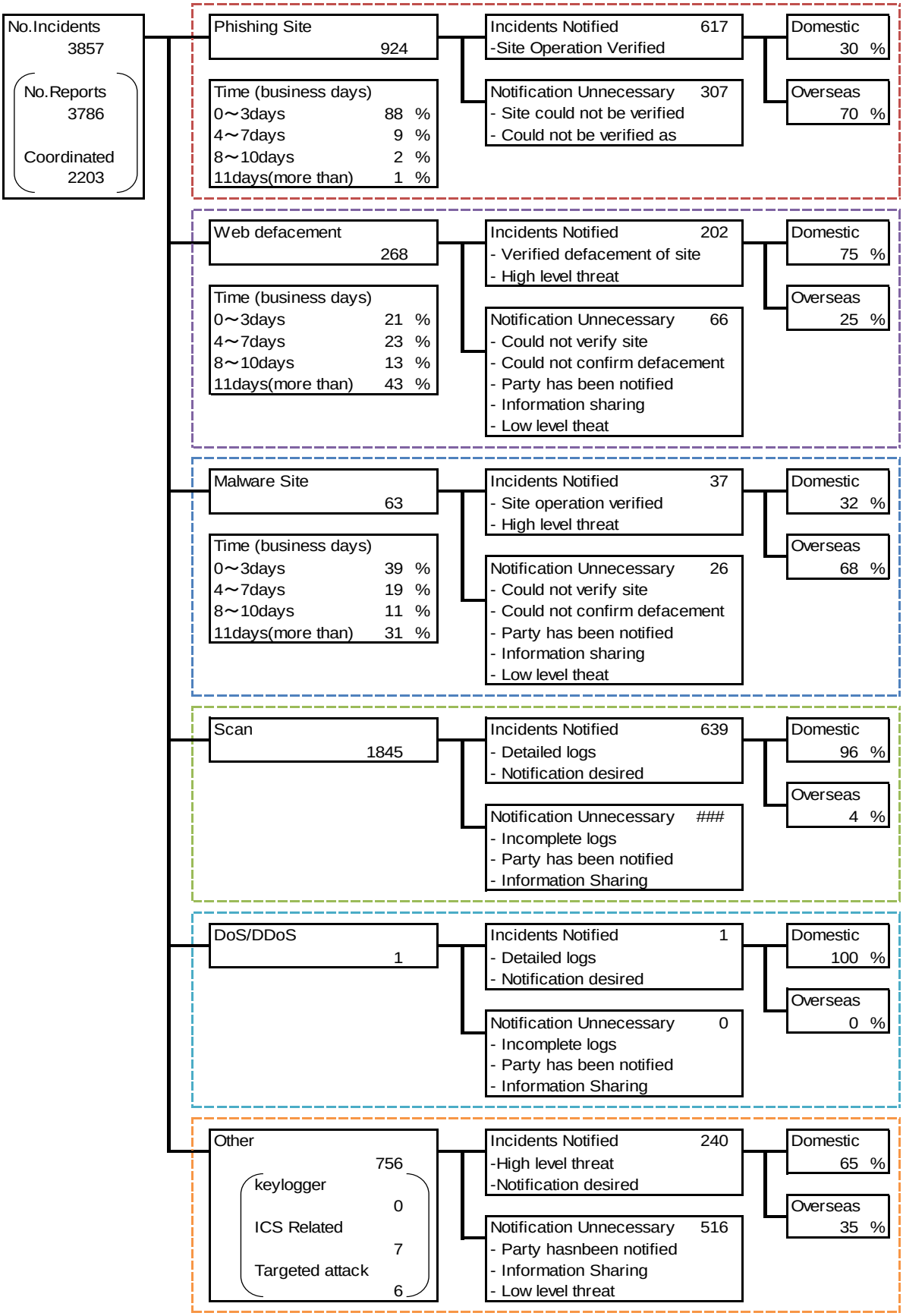


[Figure 8: Change in the number of malware sites]



[Figure 9: Change in the number of scans]

[Figure 10] provides an overview as well as a breakdown of the incidents that were coordinated / handled.



[Figure 10: Breakdown of incidents coordinated/handled]

3. Incident Trends

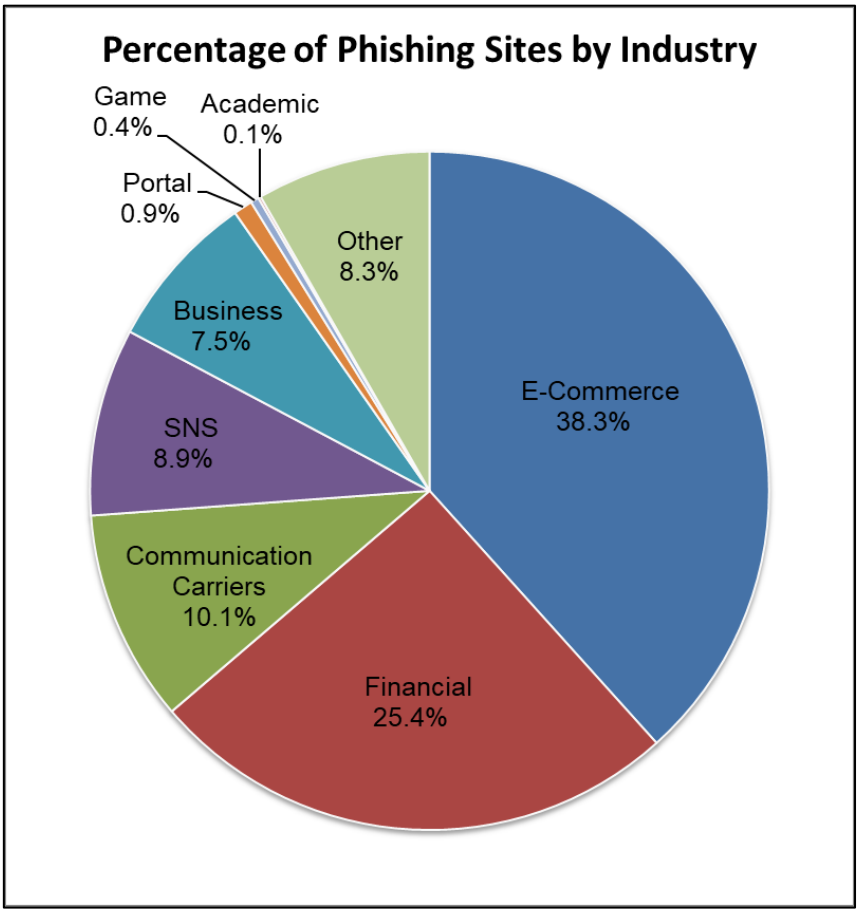
3.1. Phishing Site Trends

924 reports on phishing sites were received in this quarter, representing an 18% increase from 852 in the previous quarter. This marks a 31% increase from the same quarter last year (707). The breakdown of the brand type (domestic, overseas) that the phishing sites spoofed in this quarter is shown in [Chart5] and a breakdown by industry is shown in [Figure 11].

[Chart5: Number of reported phishing sites by domestic/overseas brand]

Phishing Site	Jan	Feb	Mar	Domestic/ Overseas Total (%)
Domestic Brand	78	58	72	208(23%)
Overseas Brand	174	212	178	564(61%)
Unknown Brand [*5]	45	41	66	152(16%)
Monthly Total	297	311	316	924(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 11: Percentage of reported phishing sites by industry]

During this quarter, there were 208 phishing sites that spoofed domestic brands, increasing 78% from 117 in the previous quarter. There were 564 phishing sites that spoofed overseas brands, decreasing 6% from 599 in the previous quarter.

Out of the total number of phishing site reports that JPCERT/CC received, 38.3% spoofed e-commerce websites, 25.4% websites of financial institutions, and 10.1% websites of telecommunications carriers.

As in the previous quarter, there were many reports regarding phishing sites designed to steal account information of specific overseas brands. JPCERT/CC confirmed multiple phishing sites that look different but actually steal account information of the same services. There were also cases in which a new phishing site with a different look was created on the same server after one phishing site was suspended, apparently indicating the presence of a common attacker.

On phishing sites of domestic brands, there were many reports regarding phishing sites spoofing telecommunications carriers, social media and financial institutions. Many of the reports on phishing sites spoofing domestic telecommunications carriers concerned two specific brands. While phishing sites spoofing one of these brands tended to be created using overseas website building services, those spoofing the other brand tended to be set up on websites using WordPress. As for phishing sites spoofing social media, this fiscal year JPCERT/CC has continually confirmed phishing sites that use a .cn domain with two or three lowercase alphabetical characters added to a brand name. Most of the phishing sites spoofing financial institutions were designed to steal credit card information.

The parties that JPCERT/CC contacted for coordination of phishing sites were 30% domestic and 70% overseas for this quarter, indicating an increase in the proportion of domestic parties compared to the previous quarter (domestic: 25%, overseas: 75%).

3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 268. This was a 3% decrease from 276 in the previous quarter.

During this quarter, JPCERT/CC confirmed compromised websites embedded with malicious JavaScript code that redirects users accessed from Google Chrome to suspicious websites or displays popups. As for defacements that display suspicious popups, in February JPCERT/CC confirmed one that convinces visitors to download and execute ransomware disguised as a Chrome font pack update. Although a similar method was confirmed around January 2017 as well, the type of ransomware that gets downloaded was different in the defacement confirmed in this quarter. The JavaScript code found embedded in multiple domestic websites in March was designed to redirect the visitor to a URL that uses an internationalized

domain name in Russian when clicked on the page. When JPCERT/CC checked these websites, however, name resolution could not be performed on the URL that the visitors were redirected to, so it was not possible to find out what kind of threat the site posed. Many of the compromised websites used CMS, so it is possible that a malicious script was embedded through an attack exploiting a vulnerability, or unauthorized login from the administration screen to plant a file.

3.3. Targeted Attack Trends

There were 6 incidents categorized as a targeted attack. This was a 23% decrease from 9 in the previous quarter. JPCERT/CC did not ask any organization to take action this quarter.

During this quarter, JPCERT/CC received information from domestic organizations about incidents such as unauthorized users logging into a cloud service that the organization uses and using the service to send fraudulent e-mail or accessing files on a cloud storage.

Some organizations that experienced similar incidents had received phishing e-mails from another domestic organization designed to direct the recipient to a phishing site spoofing the organization's authentication portal. There were also cases in which the organization sending the phishing e-mails had previously received similar phishing attacks. Investigations of organizations that had the cloud service they use accessed by unauthorized users found evidence that the attackers successfully logged in with one attempt, suggesting the possibility that account information stolen by phishing or other means may have been used.

JPCERT/CC has confirmed that unauthorized accesses were made from IP addresses of overseas hosting services and those that appear to be nodes of the anonymous network Tor. JPCERT/CC shared this IP address information with the affected domestic organizations and found that some of them were accessed from the same overseas IP addresses.

JPCERT/CC is working with organizations that had experienced similar incidents to investigate the attack and provide information to related organizations.

3.4. Other Incident Trends

The number of malware sites reported in this quarter was 63. This was a 28% decrease from 88 in the previous quarter.

The number of scans reported in this quarter was 1,845. This was a 7% decrease from 1,979 in the previous quarter. The ports that the scans targeted are listed in [Chart 6]. Ports targeted frequently were SSH (22/TCP), SMTP (25/TCP) and Telnet (23/TCP).

[Chart 6: Number of scans by port]

Port	Jan	Feb	Mar	Total
22/tcp	419	385	300	1,104
25/tcp	74	87	84	245
23/tcp	107	57	80	244
2323/tcp	41	17	33	91
80/tcp	26	15	36	77
81/tcp	2	7	8	17
445/tcp	8	4	4	16
8080/tcp	0	5	9	14
52869/tcp	5	8	0	13
3389/tcp	5	6	1	12
5555/tcp	0	4	6	10
21/tcp	7	1	2	10
82/tcp	1	0	6	7
443/tcp	3	2	2	7
2222/tcp	2	3	2	7
9999/tcp	0	0	6	6
53/udp	1	2	2	5
9000/tcp	0	4	0	4
8000/tcp	3	0	0	3
12817/udp	1	2	0	3
5912/tcp	2	0	0	2
5060/udp	1	1	0	2
44818/tcp	0	0	2	2
3333/tcp	2	0	0	2
3306/tcp	1	1	0	2
Unknown	429	632	444	1,505
Monthly Total	1,140	1,243	1,027	3,410

There were 743 incidents categorized as other. This was a 50% decrease from 1,490 in the previous quarter.

4. Incident Handling Case Examples

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

Coordination involving websites spoofing Japanese companies that victims are directed to via SMS
In early January 2018, JPCERT/CC received a number of reports about websites that spoof Japanese companies and urge visitors to install a suspicious Android application (APK file). According to the reports, SMS messages for smartphones spoofing Japanese companies were going around, trying to direct recipients to fake websites with shortened URLs. The shortened URLs direct recipients to websites that urge visitors to install an application, spoofing websites for checking the status of credit card issuance or for tracking the delivery status of parcels. A number of these websites were confirmed between early January and late February, and all of them used the same .cc domain and were assigned an IP address in Taiwan. There was also a phishing site designed to steal IDs and passwords spoofing a Japanese telecommunications carrier, using the same IP address as one of the websites distributing applications.

JPCERT/CC contacted the hosting business operator administering the servers where the websites spoofing Japanese companies were set up, and servers that the suspicious APK file communicated with, asked the operator to take appropriate steps, and confirmed that these servers have been suspended.

Coordination in response to attacks using a vulnerability in Oracle WebLogic Server
On January 17, 2018, JPCERT/CC published "Alert Regarding Vulnerability (CVE-2017-10271) in Oracle WebLogic Server." During this quarter, a number of reports concerning attacks exploiting this vulnerability have been received.

In the middle of February 2018, a report was received concerning the communication details of an attack exploiting the vulnerability in WebLogic. Upon examination of the communication log provided by the report source, JPCERT/CC found that the attack source had sent modified XML data embedded with a command to download and execute a file. In late February, a report was received concerning a file planted on a server in an attack exploiting the vulnerability in WebLogic. The files provided by the report source included a script to obtain a file from an external server and execute it, and an execution file apparently obtained by the script. The execution file was an application called XMRig, which mines a cryptocurrency called Monero. It seems the attacker was trying to obtain mining rewards.

JPCERT/CC contacted the hosting business operator that administers the server where the script and execution file used to conduct attacks were planted, informed the operator that its server was being used to carry out attacks, and requested that appropriate steps be taken.

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".