JPCERT/CC®

Japan Computer Emergency
Response Team Coordination
Center

JPCERT-IR-2014-02

Issued: 2014-04-15

JPCERT/CC Incident Handling Report[January 1, 2014 – March 31, 2014]

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 January 1, 2014 through March 31, 2014.

[*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 contact point for Japan and performs coordination with relevant parties domestically and globally (overseas CSIRTs, etc.)

2. Quarterly Statistics

[Chart1] shows the total number of incident reports, reported incidents and incidents that JPCERT/CC coordinated during this quarter.

[Chart1: Number of Incident Reports]

	Jan	Feb	Mar	Total	Last Qtr. Total
Number of Reports [* 2]	1606	1409	1883	4898	4812
Number of Incidents [* 3]	1643	1190	1696	4529	4788
Cases Coordinated [* 4]	739	614	636	1989	2135

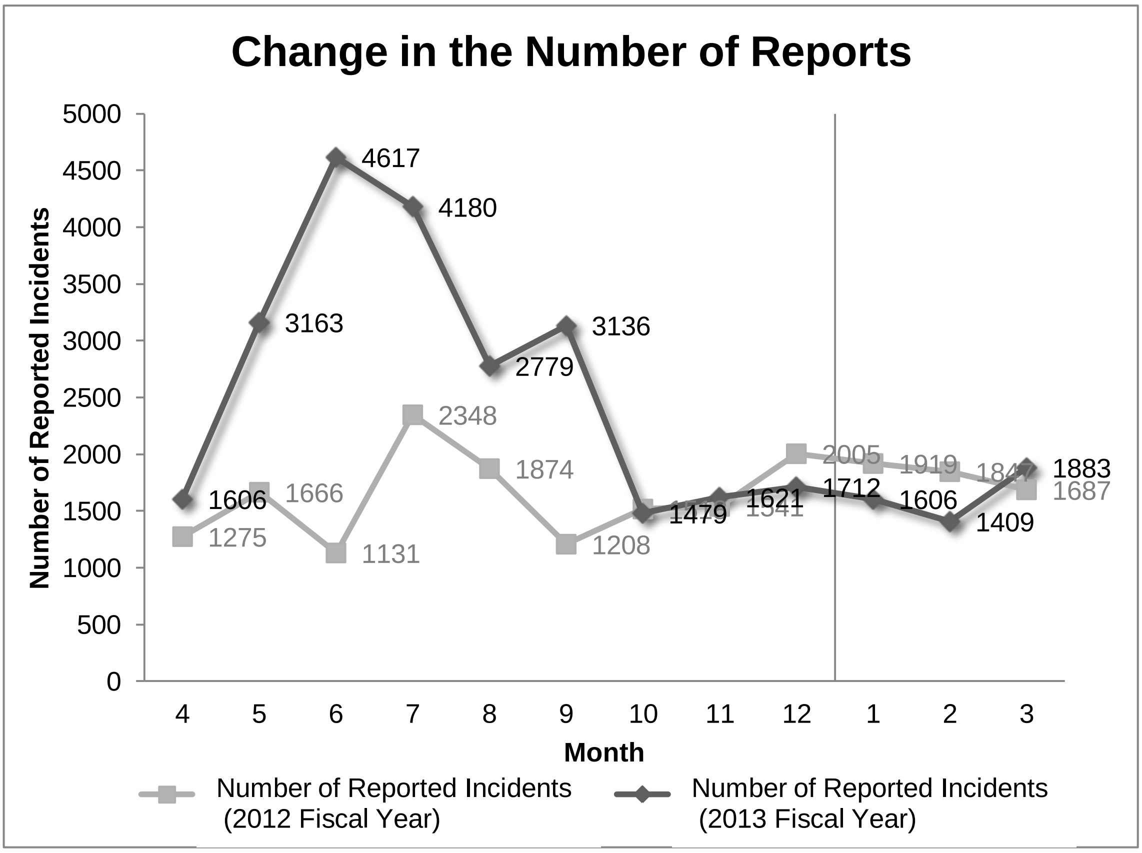
[*2] "Number of Reports" refers to the total of reports sent through the Web form, E-mail or FAX

[*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.

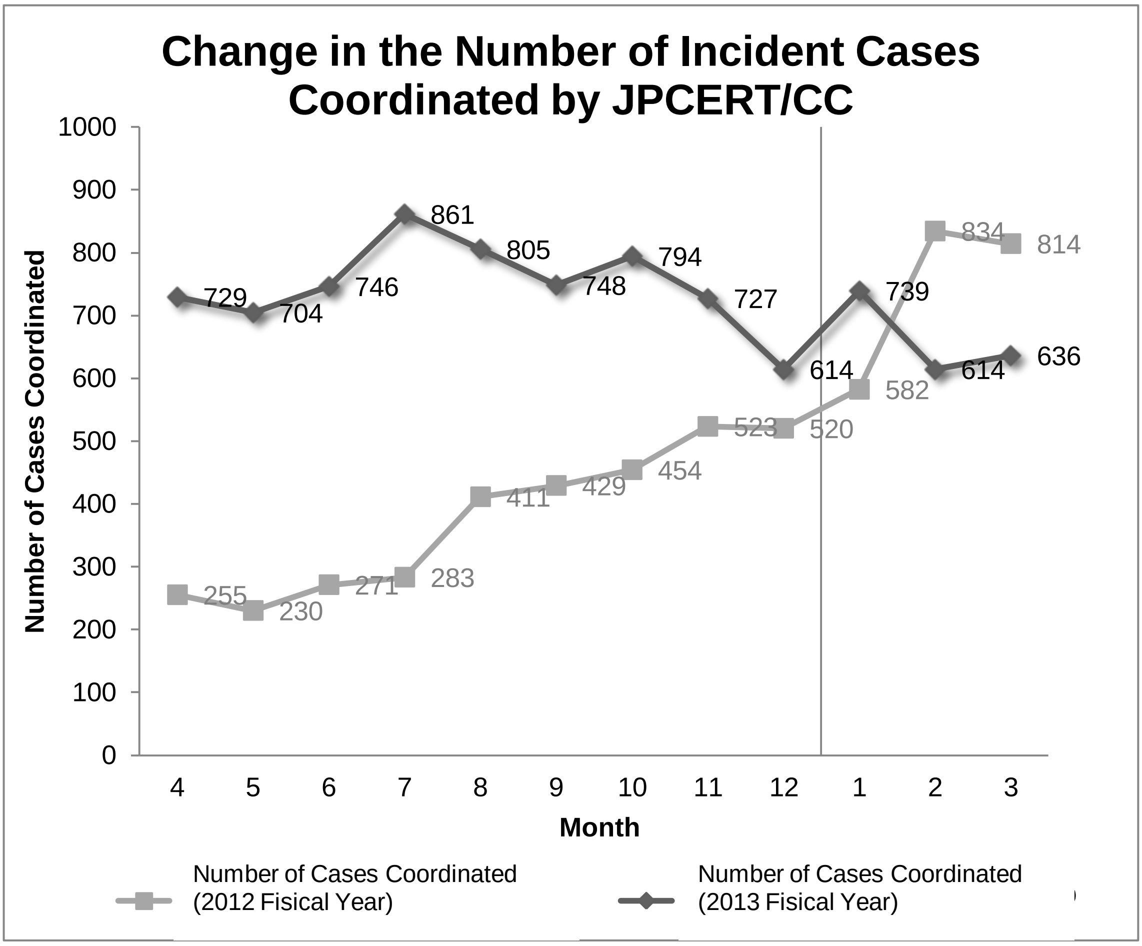
[*4] "Number of Cases Coordinated" refers to the number of cases where coordination took place to prevent the spreading of an incident by sending them a report and asking the site administrator to address any issues.

The total number of reports received in this quarter was 4,898. Out of them, the number of domestic and overseas sites that JPCERT/CC coordinated with was 1,989. When comparing this with the previous quarter, the total number of reports increased by 2%, and the number of cases coordinated decreased by 7%. When comparing with the same quarter of the previous year, the total number of reports decreased by 10%, and the number of cases coordinated decreased by 11%.

[Figure1] and [Figure2] show the monthly changes in the total number of reports and incident cases coordinated by JPCERT/CC over the past fiscal year.



[Figure1: Change in the Number of Reports]



[Figure2: Change in the Number of Incident Cases Coordinated]

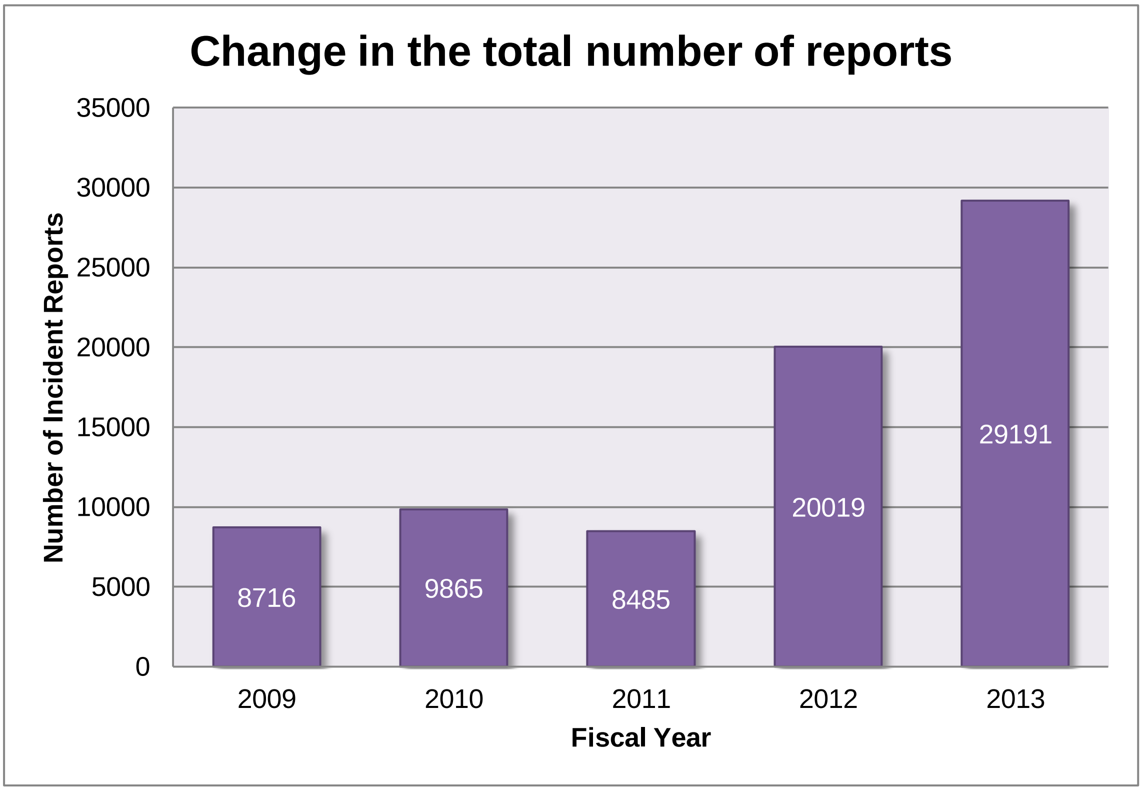
[Reference] Comparing Statistic Information by Fiscal Year

[Chart2] shows the total number of reports received during the past 5 fiscal years including the 2013 fiscal year. Each fiscal year starts on April 1st and ends the following March 31st.

[Chart2: Change in the total number of reports]

FY	2009	2010	2011	2012	2013
No. Reports	8716	9865	8485	20019	29191

The total number of reports received during the 2013 fiscal year was 29,191. This was a 46% increase from 20,019 of the previous fiscal year. [Figure3] shows the change in the total number of reports received over the past 5 years.



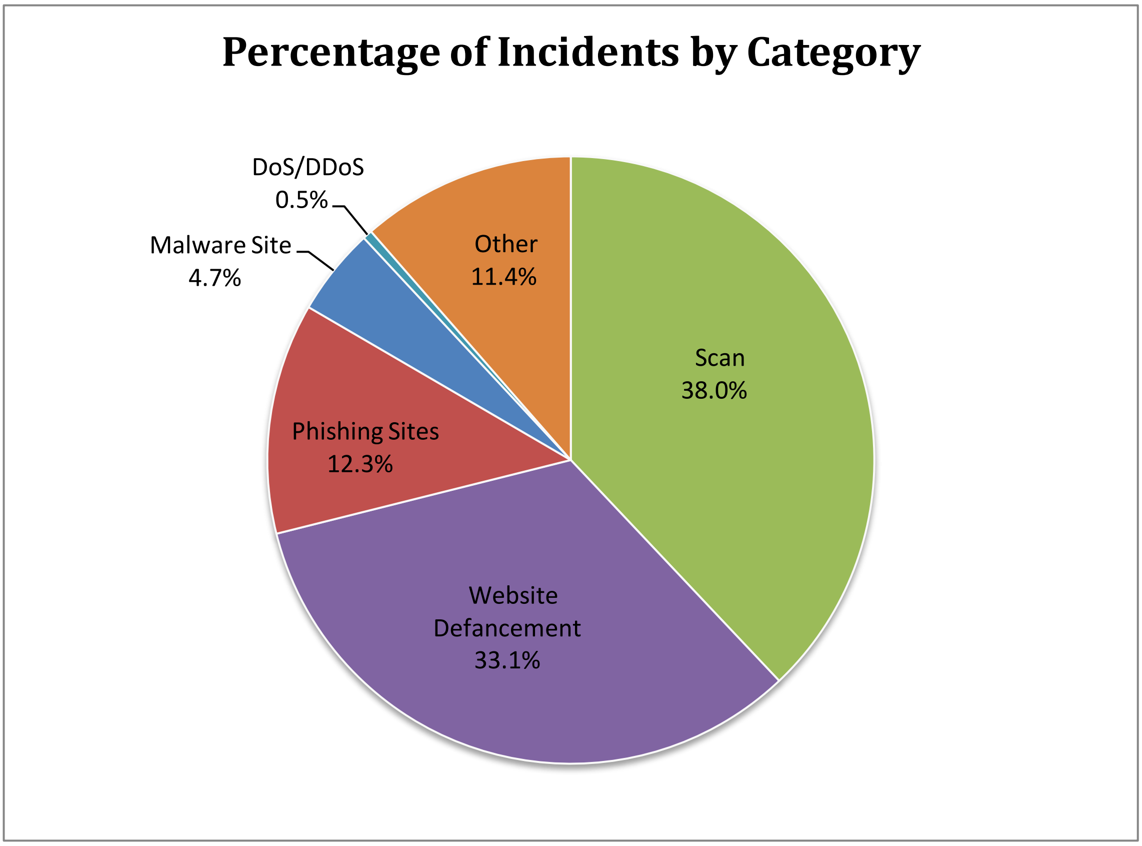
[Figure3: Change in the total number of incident reports (by fiscal year)]

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". [Chart3] shows the number of incidents received per category in this quarter.

[Chart3: Number of Incidents per Category]

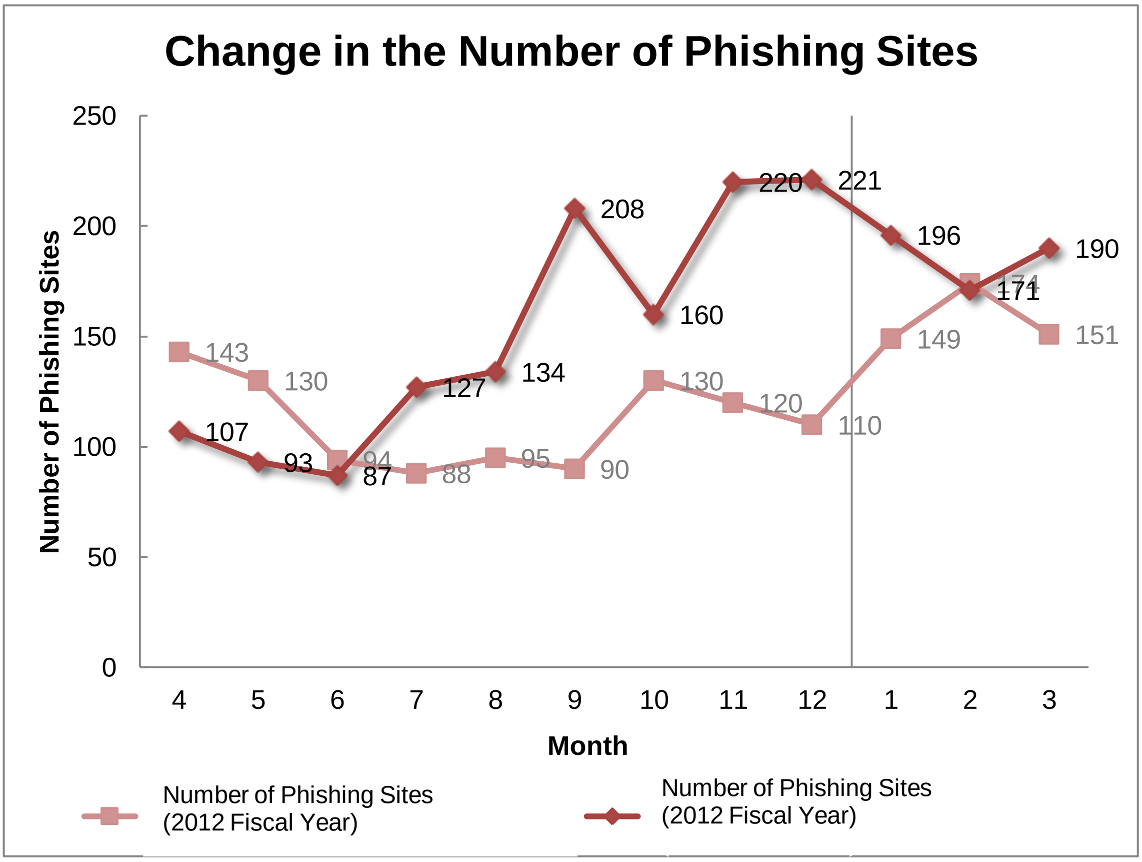
Incident Category	Jan	Feb	Mar	Total	Last Qtr. Total
Phishing Site	196	171	190	557	601
Website Defacement	663	258	580	1501	1604
Malware Site	110	46	55	211	229
Scan	417	567	735	1719	1560
DoS/DDoS	3	0	20	23	8
ICS Related	0	0	0	0	1
Other	254	148	116	518	785

The percentage that each category represents from the total number of incidents in this quarter is shown in [Figure4]. Incidents categorized as scans, which search for vulnerabilities in systems, was 38.0% and incidents categorized as website defacement was 33.1%. Also, incidents categorized as phishing sites represented 12.3% of the total.

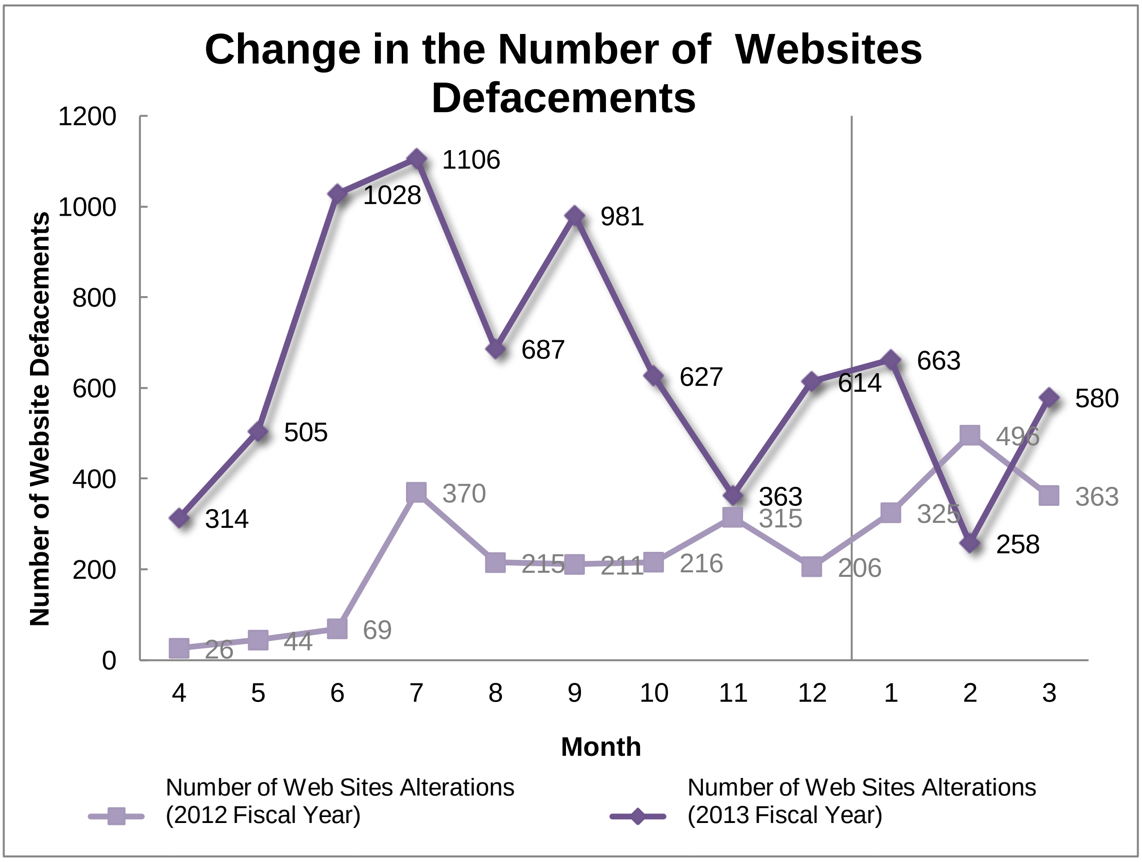


[Figure4: Percentage of Incidents by Category]

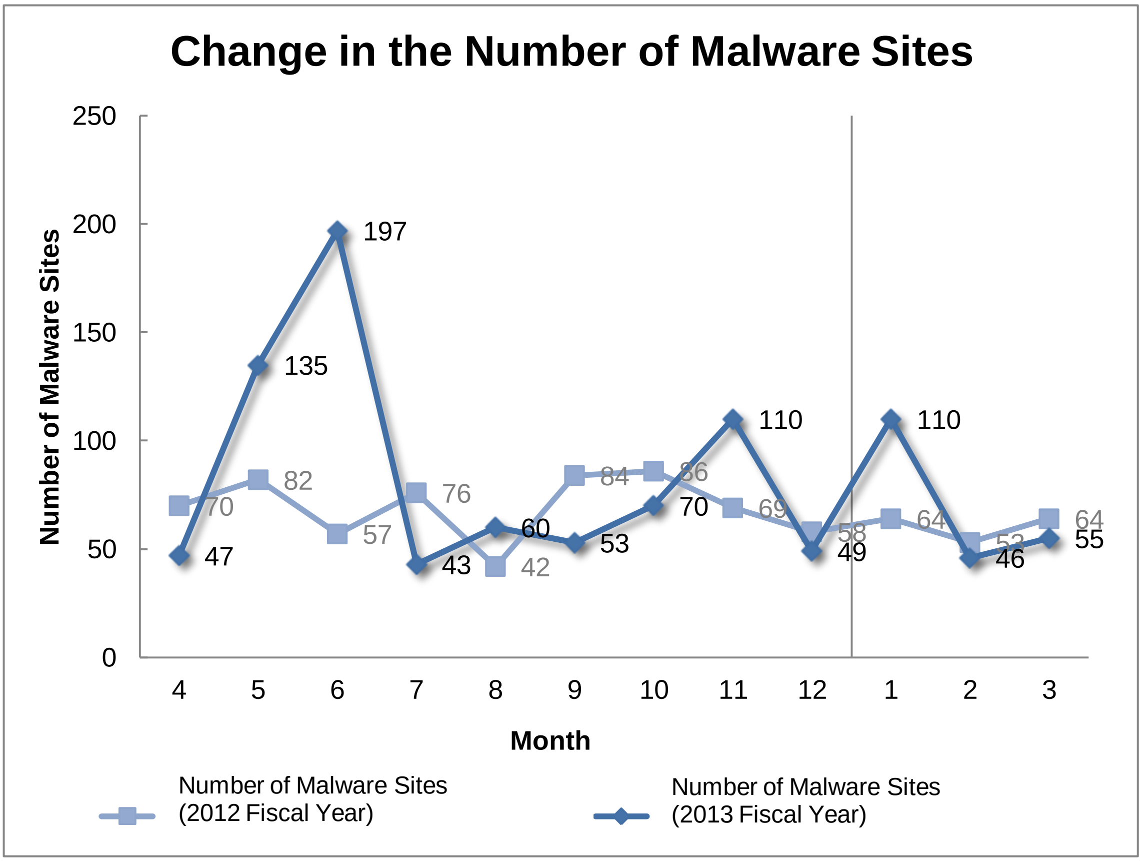
[Figure5] through [Figure8] show the monthly changes in the number of incidents categorized as phishing sites, website defacement , malware sites and scans over the past year.



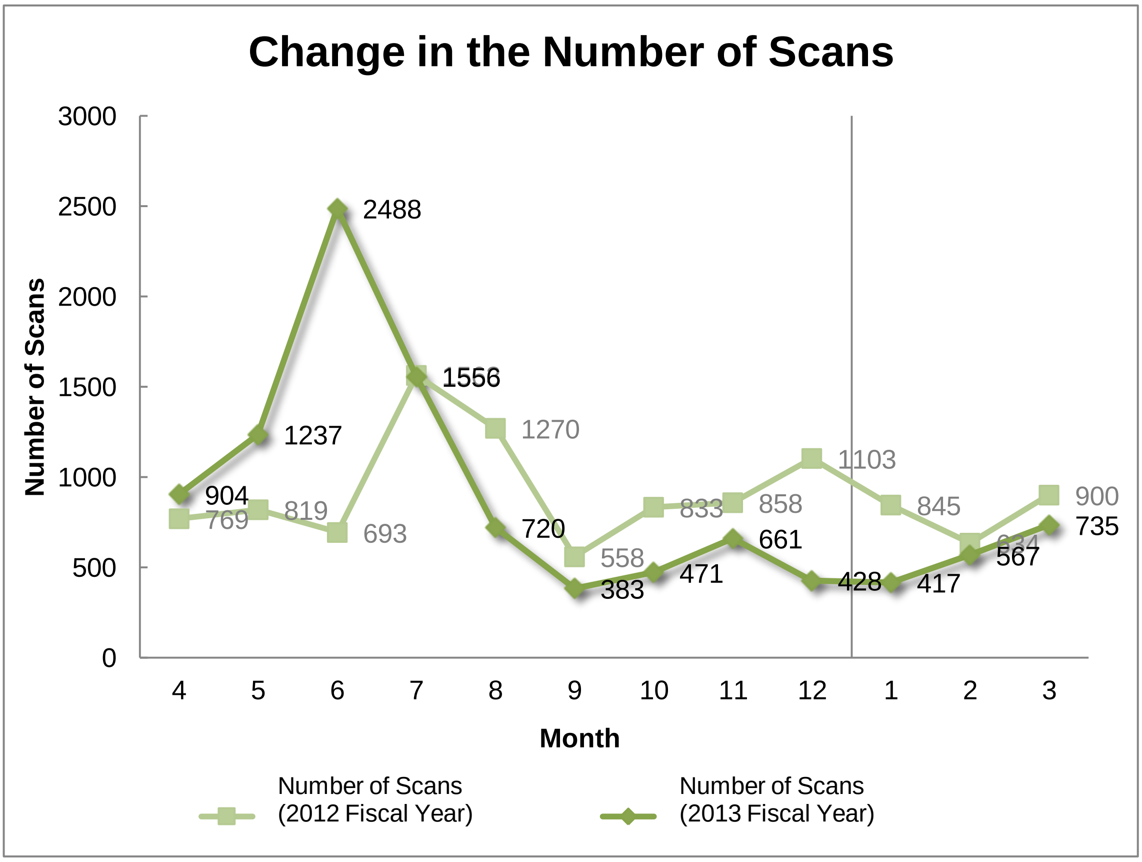
[Figure5: Change in the number of phishing sites]



[Figure6: Change in the number of website defacements]

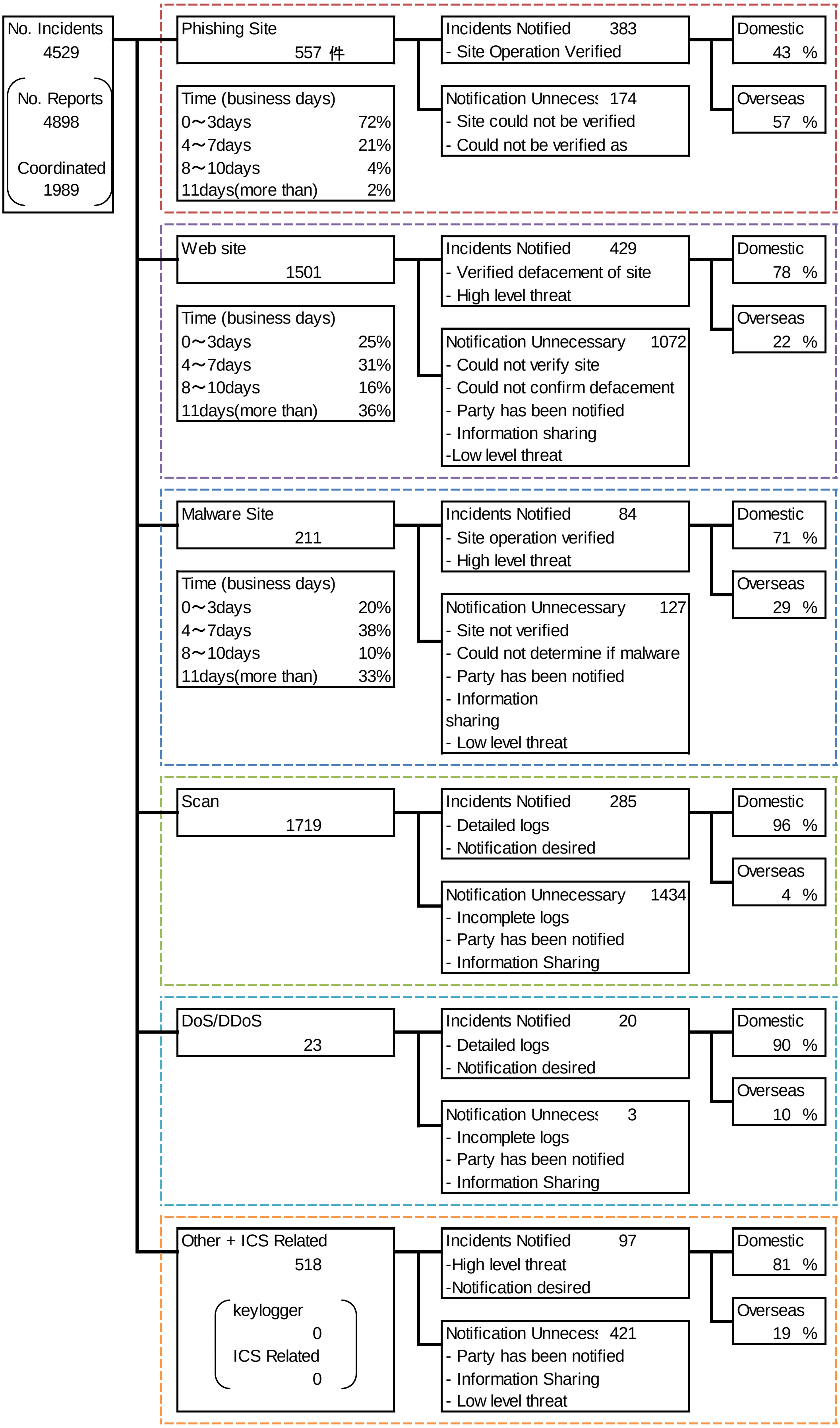


[Figure7: Change in the number of malware sites]



[Figure8: Change in the number of scans]

[Figure9] is a breakdown of the incidents that were coordinated / handled.



No. Incidents
4529

No. Reports
4898

Coordinated
1989

Phishing Site
557 件

Time (business days)

0～3days	72%
4～7days	21%
8～10days	4%
11days(more than)	2%

Incidents Notified 383
- Site Operation Verified

Notification Unneces 174
- Site could not be verified
- Could not be verified as

Domestic 43 %

Overseas 57 %

Web site
1501

Time (business days)

0～3days	25%
4～7days	31%
8～10days	16%
11days(more than)	36%

Incidents Notified 429
- Verified defacement of site
- High level threat

Notification Unnecessary 1072
- Could not verify site
- Could not confirm defacement
- Party has been notified
- Information sharing
-Low level threat

Domestic 78 %

Overseas 22 %

Malware Site
211

Time (business days)

0～3days	20%
4～7days	38%
8～10days	10%
11days(more than)	33%

Incidents Notified 84
- Site operation verified
- High level threat

Notification Unnecessary 127
- Site not verified
- Could not determine if malware
- Party has been notified
- Information sharing
- Low level threat

Domestic 71 %

Overseas 29 %

Scan
1719

Incidents Notified 285
- Detailed logs
- Notification desired

Notification Unnecessary 1434
- Incomplete logs
- Party has been notified
- Information Sharing

Domestic 96 %

Overseas 4 %

DoS/DDoS
23

Incidents Notified 20
- Detailed logs
- Notification desired

Notification Unneces 3
- Incomplete logs
- Party has been notified
- Information Sharing

Domestic 90 %

Overseas 10 %

Other + ICS Related
518

keylogger
0
ICS Related
0

Incidents Notified 97
-High level threat
-Notification desired

Notification Unneces 421
- Party has been notified
- Information Sharing
- Low level threat

Domestic 81 %

Overseas 19 %

[**Figure9: Breakdown of Incidents Coordinated / Handled**]

3.Incident Trends

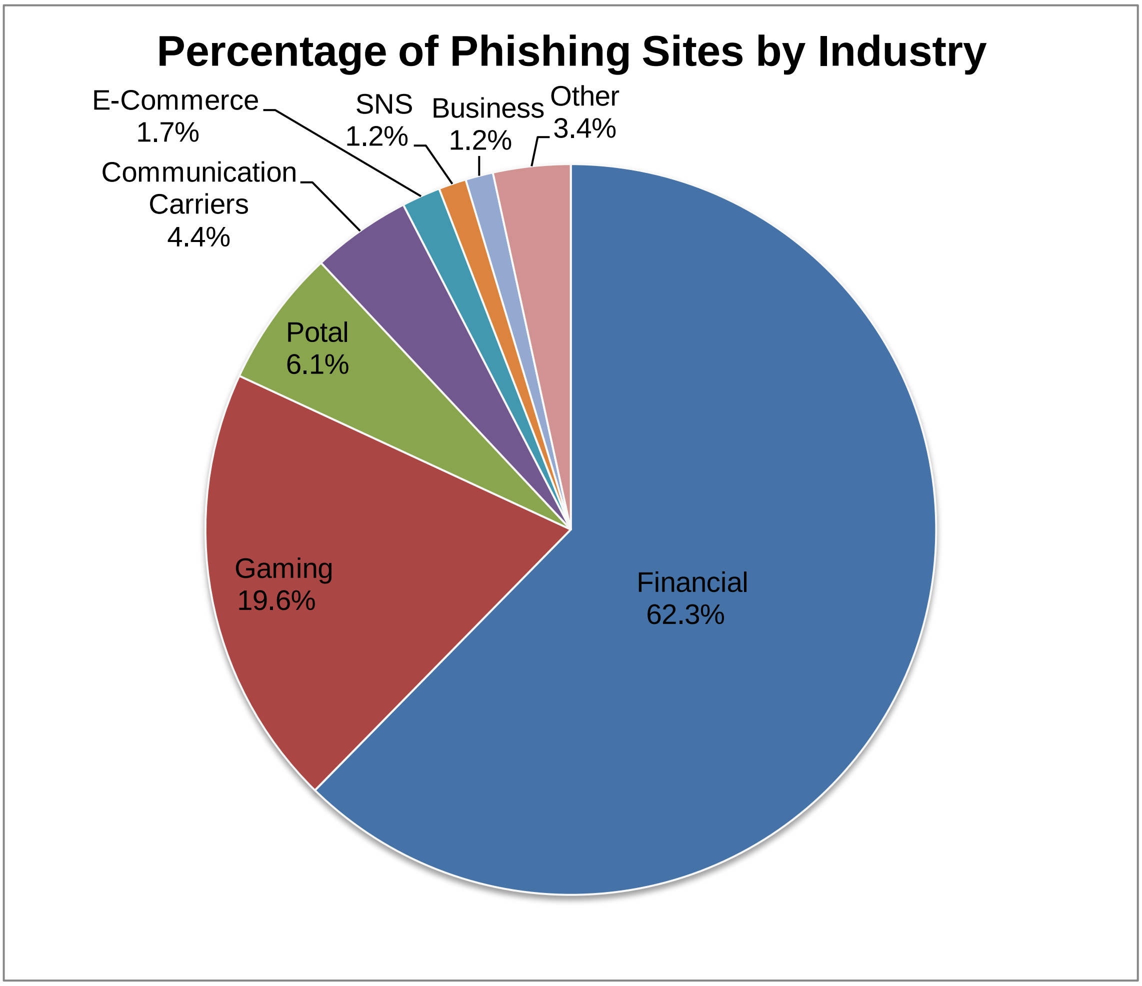
2.1. Phishing Site Trends

557 reports on phishing sites were received in this quarter, and this was a 7% decrease from 601 of the previous quarter. This number was an 18% increase from the same quarter last year (474). The breakdown of the brand type (domestic, overseas) that the phishing sites spoofed in this quarter is shown in [Chart 4], and a breakdown by industry is shown in [Figure 10].

[Chart4: Number of Phishing Sites by Domestic / Overseas Brands]

Phishing Site	Jan	Feb	Mar	Domestic / Overseas Total (%)
Domestic Brand	75	70	84	229(41%)
Overseas Brand	64	70	53	187(25%)
Unknown Brand[*5]	57	31	53	141(32%)
Monthly Total	196	171	190	557(100%)

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



[Figure10: Percentage of phishing sites by industry]

During this quarter, there were 229 phishing sites that spoofed domestic brands, which was a 9% decrease from 253 of the previous quarter. And there were 187 phishing sites that spoofed overseas brands, which was an 8% decrease from 204 of the previous quarter.

Out of the total number of phishing site reports that JPCERT/CC received, 62.3% of them spoofed sites of financial institutions, and 19.6% spoofed online gaming services. Domestically and overseas, the industry that had the most phishing sites was the financial sector.

Around mid-February, a new method was verified, where ads on search engines were leveraged to lead users to phishing sites spoofing domestic and overseas financial institutions. Since these fraudulent ads are placed at the top of the ads listings and show the legitimate URL of the financial institution, it seemed difficult for users to realize that this would lead to a phishing site just by looking at it. In order to prevent any damages that phishing sites may cause, using one-time passwords (if the financial institution provides one) or anti-phishing software is important as well as basic countermeasures such as checking if the URL is legitimate before inputting passwords or other sensitive information.

Continuing from the previous quarter, JPCERT/CC received many reports about phishing sites spoofing domestic and overseas online gaming services and domestic financial institutions, which have IP addresses dynamically assigned by domestic communications carriers. There was a period between the end of January and the second half of February where phishing sites spoofing domestic financial institutions could not be found, but after the second half of February, phishing sites being led from sites overseas were verified just like the previous quarter.

The parties that JPCERT/CC contacted for coordination of phishing sites was 43% domestic and 57% overseas for this quarter, which was the same as the previous quarter (domestic: 43%, overseas: 57%).

2.2. Website Defacement Trends

The number of website defacements reported in this quarter was 1,501. This was a 6% decrease from 1,604 of the previous quarter.

Multiple domestic websites were defaced in February 2014, and a malicious file was injected targeting at vulnerability in Internet Explorer (CVE-2014-0322) which had not been fixed at the time. The defaced website would lead users to a swf file or a jar file that attacks the vulnerability via an embedded iframe or JavaScript to infect the user PC with malware. After analyzing the malware that the attacks used, its malicious behavior was revealed including sending device information to overseas servers and retrieving data by accessing a specific page provided by a domestic blog service which the attackers supposedly had been sending commands to the malware from.

In addition, a large number of reports about websites that have malicious iframe or JavaScript embedded were also received.

2.3. Other Incident Trends

The number of malware sites reported in this quarter was 211. This was an 8% decrease from 229 of the previous quarter.

The number of scans reported in this quarter was 1,719. This was a 10% increase from 1,560 of the previous quarter. The ports that the scans targeted are listed in [Chart 5]. Ports targeted frequently were smtp(25/tcp), http(80/tcp) and ssh(22/tcp).

[Chart5: Number of Scans by Port]

Port	Jan	Feb	Mar	Total
25/tcp	193	318	342	853
80/tcp	156	180	300	636
22/tcp	79	54	50	183
udp	4	40	29	73
21/tcp	3	2	16	21
23/tcp	0	2	10	12
3389/tcp	1	5	5	11
143/tcp	1	5	2	8
5900/tcp	3	2	1	6
5000/tcp	0	0	5	5
1433/tcp	4	1	0	5
8080/tcp	1	0	1	2
443/tcp	2	0	0	2
3306/tcp	0	0	2	2
135/tcp	0	2	0	2
9090/tcp	0	0	1	1
7822/tcp	1	0	0	1
6000/tcp	0	0	1	1
5631/tcp	1	0	0	1
50000/tcp	0	0	1	1
500/tcp	1	0	0	1
25724/tcp	0	1	0	1
Unknown	13	12	8	33
Month Total	463	624	774	1861

3. Incident Handling Case Examples

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

[Coordination for domestic NTP servers abused in DDoS attacks overseas]
JPCERT/CC issued an alert regarding DDoS attacks leveraging the monlist function of ntpd in the middle of January. Since NTP uses UDP for communications, the source IP can be spoofed for requests. Also, the monlist function in ntpd responds with a packet larger in size than the request packet. Thus, an attacker can set the victim IP address as the source address and send a monlist request to the NTP server to send the victim data that is large in size.

From January 2014 to February 2014, multiple overseas organizations reported that they had observed DDoS attacks from NTP servers located in some Japanese domestic network. JPCERT/CC checked whether the monlist function in ntpd was enabled for the reported IP address, and for the ones that were enabled, we asked the host's network administrator to change the settings.

[Coordination involving domestic hosts infected by SSH rootkits]
At the beginning of January 2014, an overseas National CSIRT reported about domestic hosts that was infected by a SSH rootkit. This is malware that steals and sends SSH account information and private keys to an external server. The reporting organization sent communication records between the server where the stolen information was being sent to and the domestic host. This SSH rootkit had a characteristic that uses a large area of internal memory space where all users could read and write to, and this needs to be checked for confirming the infection.
Based on the reported information, JPCERT/CC contacted the network administrator of the server in question to notify the possibility of SSH root infection and how to check for the infection.

[Assistance in anti-botnet project conducted by Microsoft and an overseas CSIRT]
JPCERT/CC received C&C (Command and Control Server) logs from CNCERT/CC, (the national CSIRT of China), which they obtained through a project against a botnet “Nitol” in cooperation with Microsoft. Computers infected by Nitol are remotely controlled by a malicious third party, and stored information is stolen.

Based on the logs provided, we asked the network administrator of the server to investigate whether there were access attempts to the C&C at the time shown in the logs and if the host in question was infected by malware. Some organizations responded about their infection by Nitol and other malware. JPCERT/CC cooperated in CNCERT/CC’s anti-botnet project by sharing the infection report with them (with approval from the reporters).

Request from JPCERT/CC

JPCERT/CC attempts to prevent the spread of damages caused by incidents and the recurrence of incidents by understanding the occurrence and trends and also contacting the source of the attack to coordinate in suspending the websites depending on the circumstances. Issuing alerts to notify users to apply countermeasures is also a part of our activities.

JPCERT/CC highly appreciate your cooperation in reporting any information; please refer to the following URLs on how report incidents.

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

If you would like to encrypt your report, please use JPCERT/CC's PGP public key from the following URL.

Public Key
https://www.jpcert.or.jp/keys/info-0x69ECE048.asc

PGP Fingerprint：
FC89 53BB DC65 BD97 4BDA D1BD 317D 97A4 69EC E048

Appendix 1: Incident Categories

JPCERT/CC defines each incident included in the reports as follows:

○ Phishing Site

A "Phishing Site" refers to a site that spoofs a legitimate site provided by a service provider (of banks, auction websites etc.), which intends to obtain user ID's, passwords, credit card numbers, etc. for "phishing fraud" purposes.

JPCERT/CC categorizes the following as "phishing sites"

- Websites that imitate websites of financial institutions, credit card companies etc.
- Websites aimed at leading users to phishing sites

○ Website Defacement

"Website Defacement" refers to a website where the contents have been re-written (including embedding of scripts not intended by the administrator) by an attacker or malware.

JPCERT/CC categorizes the following as "website defacement"

- Websites where malicious scripts or iframes are embedded by an attacker or malware
- Websites where information has been altered as a result of an SQL injection attack

○ Malware Site

"A Malware Site" refers to a website where a PC may be infected by malware when viewing the site or a website that hosts malware for an attack.

JPCERT/CC categorizes the following as "malware site"

- Websites that attempt to infect its visitors' PC with malware
- Websites where malware is hosted by an attacker

○ Scan

"Scan" refers to access by attackers (that do not affect the system) to search for vulnerabilities (security holes, etc.) in a server, PC or any system targeted for an attack to gain unauthorized access. Attempts to infect with malware are also included here.

JPCERT/CC categorizes the following as "scan"

- Vulnerability searching (checking program versions, service operation etc.)
- Attempts at intrusion (that do not result in intrusion)
- Attempts (that do not result in infection) to infect with malware (virus, bots, worms, etc.)
- Brute force attacks against ssh, ftp, telnet, etc. (that do not result in successful attack)

○ DoS/DDoS

"DoS / DDoS" refers to an attack against network resources of servers, PC's and other devices that form the network, which results in not being able to provide services.

JPCERT/CC categorizes the following as "DoS / DDoS"

- Attacks that exhaust network resources as a result of large number of communications
- Bad response or suspension of server programs due to large amount of access
- Interference of services by forcing reception of a large number of e-mails (error e-mails, spam e-mails, etc.)

○ ICS Related Incidents

"ICS Related Incidents" refer to any incidents related to industrial control systems or any type of plant.

JPCERT/CC categorizes the following as "ICS related incidents"

- Industrial control systems that can be attacked over the internet
- Servers that communicate with malware targeting control systems
- Attacks that cause malfunctioning of industrial control system

○ Other

"Other" refers to incidents that cannot be categorized in any of the above.

For example, JPCERT/CC categorizes the following as "other"

● Unauthorized intrusions into a system leveraging a vulnerability

● Unauthorized intrusion as a result of a successful brute force attack against ssh, ftp, telnet, etc.

● Information stealing by malware that contains a key logging function

● Malware (virus, bots, worms, etc.) infections

These activities are sponsored by the Ministry of Economy, Trade and Industry as part of the "Information Security Countermeasure Promotion Activities for the 2013 Fiscal Year".