JPCERT/CC®

Japan Computer Emergency
Response Team Coordination
Center

JPCERT-IR-2016-04

Issued: 1/11/2017

JPCERT/CC Incident Handling Report
[October 1, 2016 - December 31, 2016]

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, 2016 through December 31, 2016.

(*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	1150	1273	1613	4036	3137
Number of Incident *3	1281	1409	1432	4122	2801
Cases Coordinated *4	1038	1048	797	2883	2122

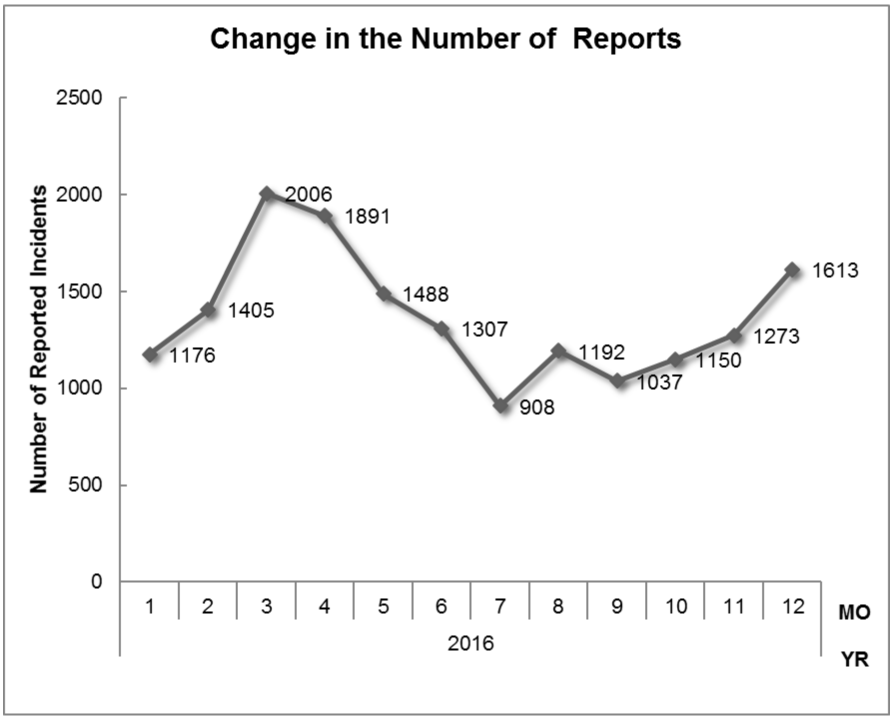
(*2) "Number of Reports" refers to the total number of reports sent through the web form, e-mail or FAX.

(*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.

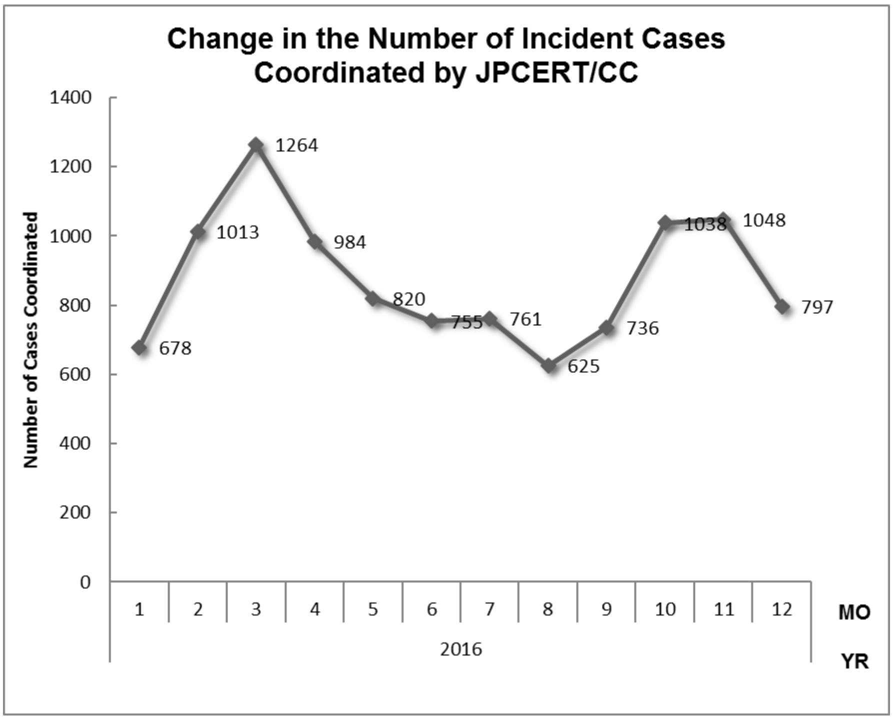
(*4) "Number of Cases Coordinated" refers to the number of cases where coordination took place to prevent the spreading of an incident by sending them a report and asking the site administrator to address any issues.

The total number of reports received in this quarter was 4,036. Of these, the number of domestic and overseas sites that JPCERT/CC coordinated with was 2,883. When compared with the previous quarter, the number of reports increased 29%, and the number of cases coordinated increased 36%. Year on year, the number of reports increased 17%, and the number of cases coordinated increased 40%.

[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 Reports]



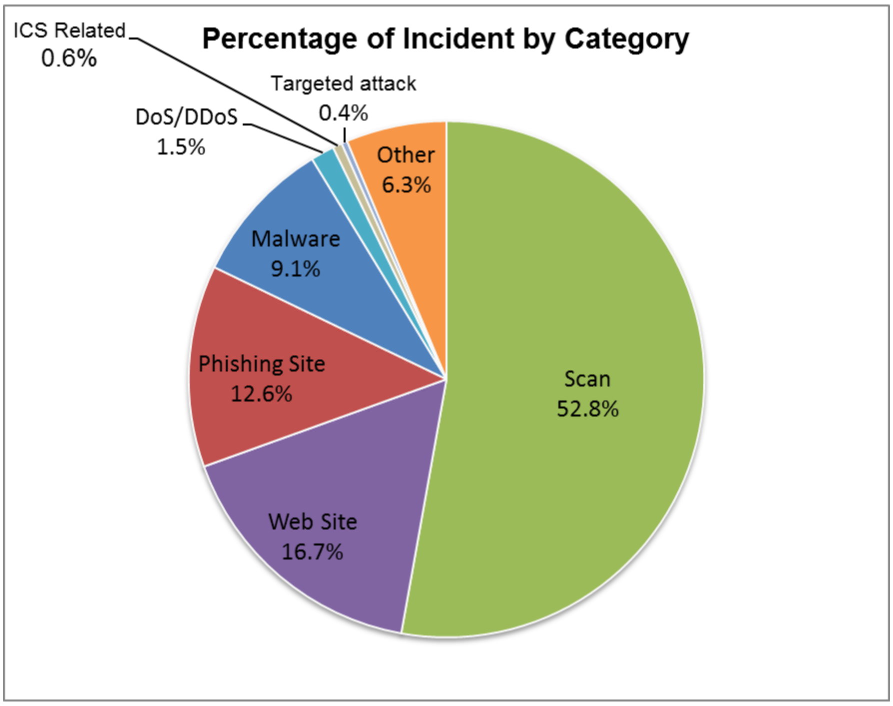
[Figure 2: Change in the Number of Incident Cases Coordinated]

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 per Category]

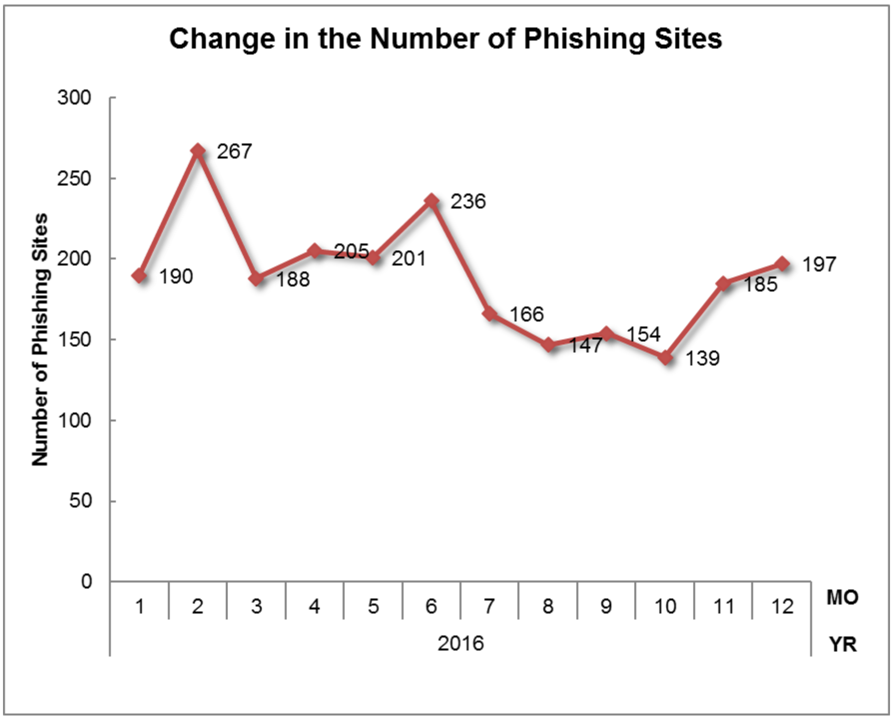
Incident Category	Oct	Nov	Dec	Total	Last Qtr. Total
Phishing Site	139	185	197	521	467
Website Defacement	180	314	194	688	554
Malware Site	110	116	150	376	337
Scan	709	679	789	2177	1098
DoS/DDoS	59	2	0	61	54
ICS Related	3	13	8	24	5
Targeted attack	8	4	3	15	10
Other	73	96	91	260	276

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 52.8%, and incidents categorized as website defacement made up 16.7%. Also, incidents categorized as phishing sites represented 12.6% of the total.

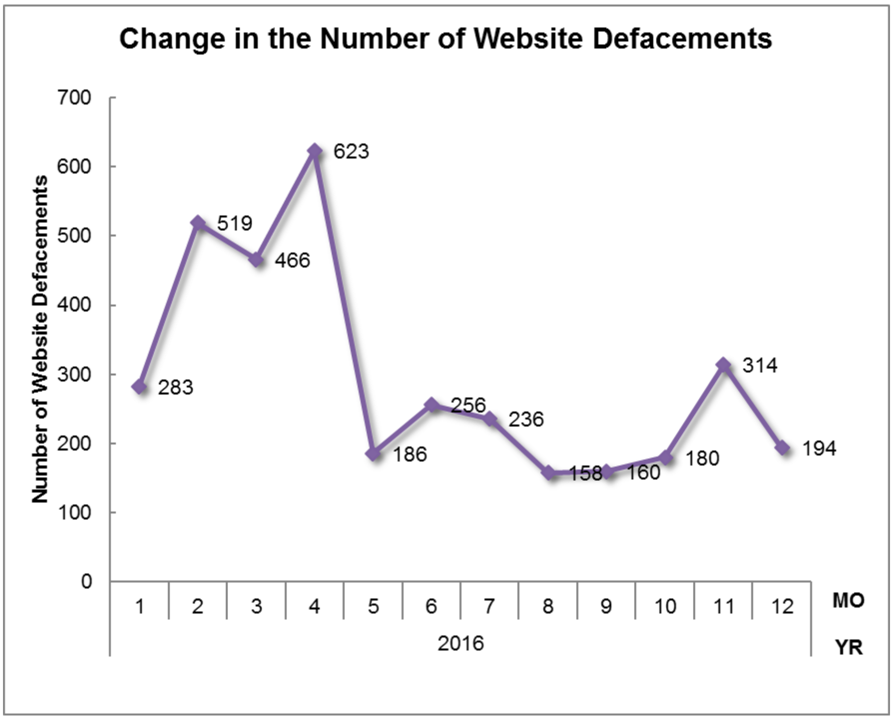


[Figure 3: Percentage of incidents by category]

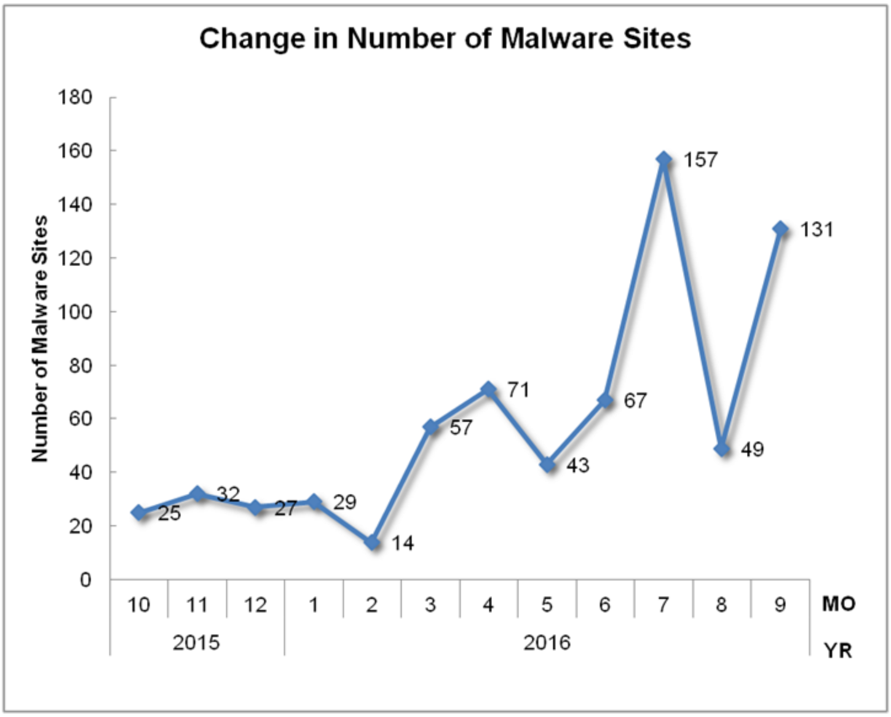
[Figure 4] through [Figure 7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



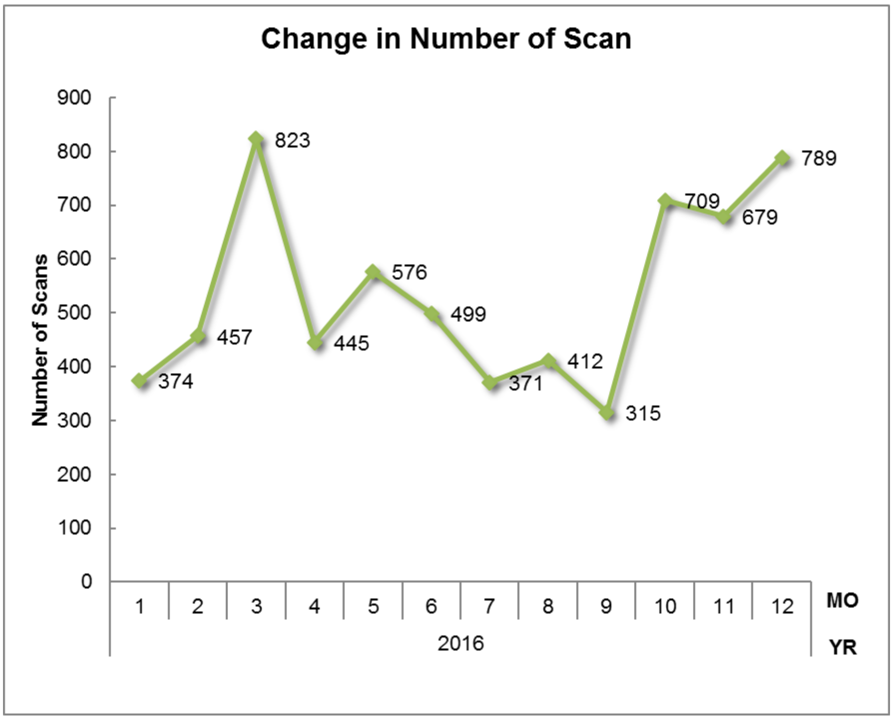
[Figure 4: Change in the number of phishing sites]



[Figure 5: Change in the number of website defacements]

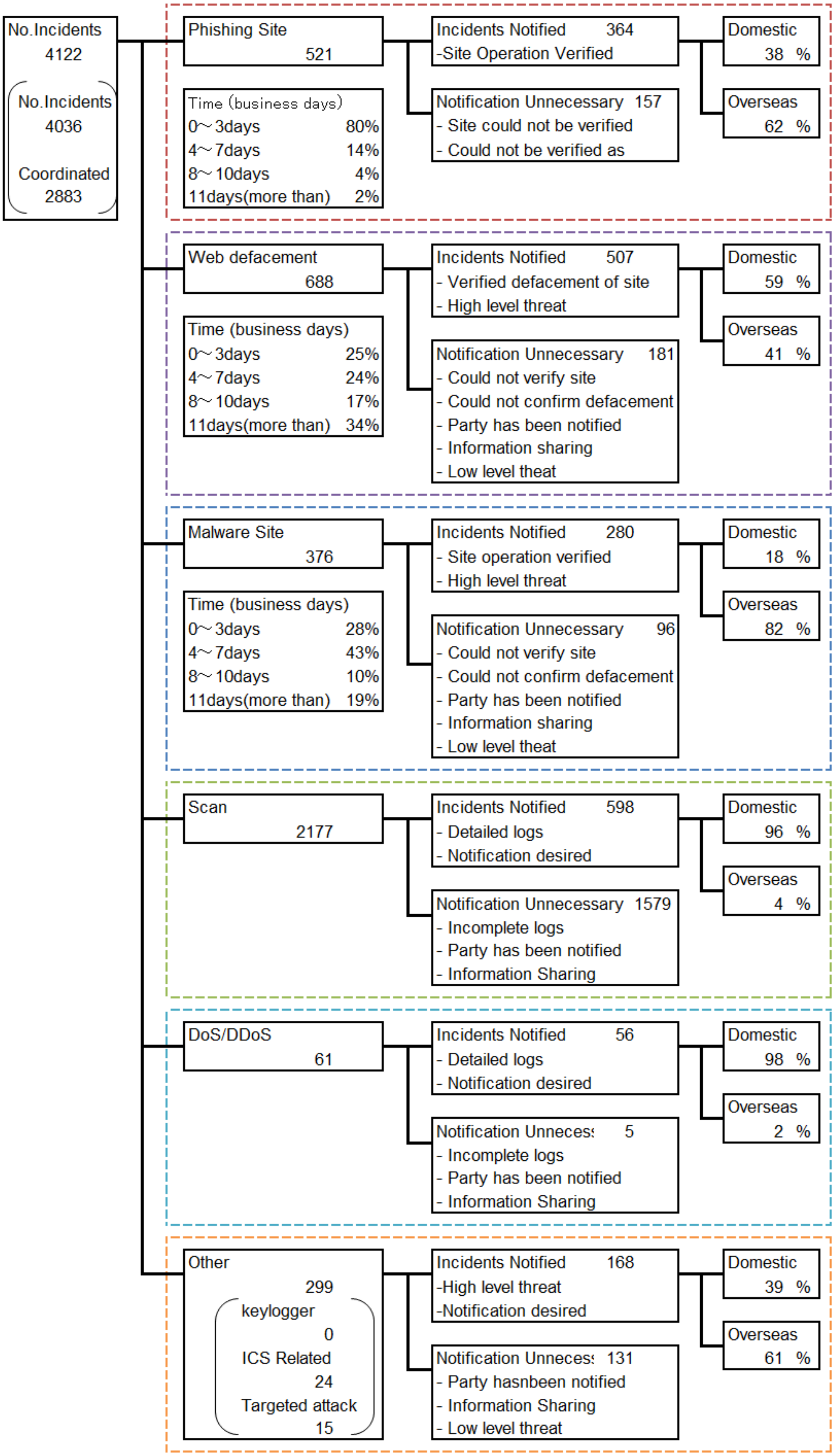


[Figure 6: Change in the number of malware sites]



[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.



No.Incidents 4122

(No.Incidents 4036
Coordinated 2883)

Phishing Site 521

Time (business days)	
0～3days	80%
4～7days	14%
8～10days	4%
11days(more than)	2%

Incidents Notified 364
-Site Operation Verified

Notification Unnecessary 157
- Site could not be verified
- Could not be verified as

Domestic 38 %

Overseas 62 %

Web defacement 688

Time (business days)	
0～3days	25%
4～7days	24%
8～10days	17%
11days(more than)	34%

Incidents Notified 507
- Verified defacement of site
- High level threat

Notification Unnecessary 181
- Could not verify site
- Could not confirm defacement
- Party has been notified
- Information sharing
- Low level theat

Domestic 59 %

Overseas 41 %

Malware Site 376

Time (business days)	
0～3days	28%
4～7days	43%
8～10days	10%
11days(more than)	19%

Incidents Notified 280
- Site operation verified
- High level threat

Notification Unnecessary 96
- Could not verify site
- Could not confirm defacement
- Party has been notified
- Information sharing
- Low level theat

Domestic 18 %

Overseas 82 %

Scan 2177

Incidents Notified 598
- Detailed logs
- Notification desired

Notification Unnecessary 1579
- Incomplete logs
- Party has been notified
- Information Sharing

Domestic 96 %

Overseas 4 %

DoS/DDoS 61

Incidents Notified 56
- Detailed logs
- Notification desired

Notification Unneces 5
- Incomplete logs
- Party has been notified
- Information Sharing

Domestic 98 %

Overseas 2 %

Other 299

(keylogger 0
ICS Related 24
Targeted attack 15)

Incidents Notified 168
-High level threat
-Notification desired

Notification Unneces 131
- Party hasnbeen notified
- Information Sharing
- Low level threat

Domestic 39 %

Overseas 61 %

[Figure 8: Breakdown of incidents coordinated/handled]

3. Incident Trends

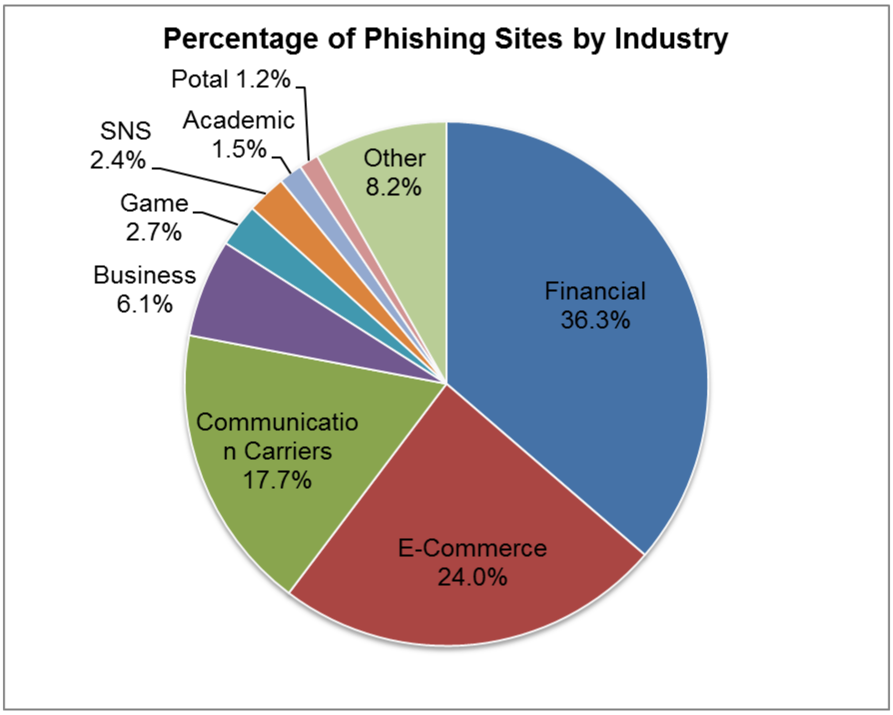
3.1. Phishing Site Trends

521 reports on phishing sites were received in this quarter, representing a 12% increase from 467 of the previous quarter. This marks a 10% 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 3], and a breakdown by industry is shown in [Figure 9].

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

Phishing Site	Oct	Nov	Dec	Domestic/ Overseas Total (%)
Domestic Brand	24	47	63	134(26%)
Overseas Brand	88	106	85	279(54%)
Unknown Brand (*5)	27	32	49	108(21%)
Monthly Total	139	185	197	521(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 phishing sites by industry]

During this quarter, there were 134 phishing sites that spoofed domestic brands, increasing 26% from 106 of the previous quarter. And there were 279 phishing sites that spoofed overseas brands, increasing 15% from 243 of the previous quarter.

Out of the total number of phishing site reports that JPCERT/CC received, 36.3% spoofed websites of financial institutions, and 24.0% spoofed e-commerce websites.

As for phishing sites spoofing domestic brands, many of the reported cases aimed at stealing information of web-based e-mail accounts, continuing the trend seen in the previous quarter. Since the end of October, JPCERT/CC has continuously confirmed phishing sites spoofing the login screen of a domestic carrier's web-based e-mail. These phishing attacks tended to use a shortened URL included in an e-mail message to direct the recipient to the actual phishing site. At the end of October and in late November, JPCERT/CC also received reports of phishing sites spoofing the login screen of the web-based e-mail of a number of domestic universities. Since some of these universities used the same free overseas website building service, these phishing attacks could have been perpetrated by the same attacker.

As for phishing sites spoofing online gaming services, changes were observed in the affected brands and the hosting services where the websites were set up between October and November onwards. However, most of the phishing sites used a free .cc domain as in the previous quarter.

While many phishing sites of domestic financial brands were attempting to steal credit card information, there were only a few phishing sites spoofing banks.

The parties that JPCERT/CC contacted for coordination of phishing sites were 38% domestic and 62% 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 688, increasing 24% from 554 of the previous quarter.

JPCERT/CC received information about defacements in which a script that loads a malicious PHP file named index_old.php is embedded in the top page of the website. In response, JPCERT/CC published an "Alert regarding website defacements" on November 14. Once this malicious PHP file gets loaded, the IP address, the browser's user agent, access time and other information are logged, allowing such information to be collected for use in attacks.

As in the previous quarter, JPCERT/CC received numerous reports of website defacements, and many of the compromised websites used WordPress or other CMSs. Furthermore, there were reports that numerous domestic e-commerce websites using a CMS called Magento were embedded with a script designed to steal credit card numbers and other information. JPCERT/CC investigated each website and found that a number of them were embedded with the malicious script. The administrators of the compromised websites were duly requested to address the problem.

3.3. Targeted Attack Trends

There were 15 incidents categorized as a targeted attack. JPCERT/CC requested a total of 7 organizations to take action during this quarter.

JPCERT/CC is continuing to address the advanced targeted attacks using a large number of C2 servers that were discussed in the previous quarter's Incident Handling Report. During this quarter, requests were made to administrators of equipment used as C2 servers for the malware used in this series of attacks to investigate the equipment and to capture and submit files and programs placed by the attackers.

In some of the cases where data were provided, there were no program files corresponding to the URL specified as the malware's communication destination, and there were also cases in which no suspicious signs of alteration were found in existing program files, even though signs of intrusion by an attacker remained. These could have been cases in which the attacker made preparations to exploit the equipment as a C2 server but never actually used it.

During this quarter, there were also a number of reports concerning spoofed e-mail with malware attached. Incidents of e-mail spoofing reported in late October involved attachment of a type of malware called downloader. JPCERT/CC confirmed that it downloads another type of malware from the host at the IP address that was confirmed at the end of August to be the communication destination for remote control malware called PlugX.

In late November, there were reports of spoofed e-mails with a zip file attached containing a PDF file and an execution file. JPCERT/CC analyzed this execution file and found that it was a type of remote control malware that operates by receiving external commands. It was also found that this malware communicated with the same server as the malware that was attached to a spoofed e-mail sent to another domestic organization around the same time. This finding points to the possibility that a number of domestic organizations were subjected to similar attacks within the same timeframe.

3.4. Other Incident Trends

The number of malware sites reported in this quarter was 376. This was a 12% increase from 337 of the previous quarter.

The number of scans reported in this quarter was 2,177. This was a 98% increase from 1,098 of the previous quarter. The ports that the scans targeted are listed in [][Chart 4]. Ports targeted frequently were SSH (22/TCP), SMTP (25/TCP) and HTTP (80/TCP).

[Chart 4: Number of scans by port]

Port	Oct	Nov	Dec	Total
22/tcp	255	186	260	701
25/tcp	156	161	286	603
80/tcp	70	205	161	436
53/udp	128	61	24	213
23/tcp	28	31	33	92
21/tcp	35	33	0	68
2323/tcp	9	16	6	31
5358/tcp	0	0	11	11
3389/tcp	2	4	2	8
5060/udp	0	0	6	6
33442/udp	2	0	3	5
23887/udp	0	2	3	5
4752/udp	2	1	1	4
81/tcp	0	2	1	3
554/tcp	0	2	1	3
2222/tcp	0	0	3	3
143/tcp	1	1	1	3
51331/udp	2	0	0	2
445/tcp	0	2	0	2
30586/udp	1	1	0	2
137/udp	2	0	0	2
Other	242	161	197	600
Monthly Total	935	869	999	2,803

There were 260 incidents categorized as other. This was a 6% decrease from 276 of the previous quarter.

4. Incident Handling Case Examples

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

[Defacement of websites using WordPress or other CMSs]

Among the website defacements confirmed during this quarter, there were a number of cases in which an obfuscated JavaScript code is embedded at the foot of a legitimate web page when first accessed, but only the legitimate web page is returned when subsequently accessed from the same IP address. According to the administrators of some of the compromised websites, most of the PHP files of the CMS they used had a suspicious code embedded at the top. This suspicious code was designed to capture the IP address of the computer from which the website was accessed and send it to a C2 server, which would then send back a response. Based on this response, the code determines whether to embed a malicious JavaScript or return the legitimate web page. There were also cases in which a backdoor was planted to execute any PHP code.

Around the end of November, there was a report of a case in which a script containing strings such as jquery.min.php was embedded in a PHP file named header.php, which is used as a CMS template file. The reporter claimed that the script gets embedded repeatedly no matter how many times correction was made. A number of suspicious PHP files were also planted, including webshells, which attackers use to control a server via the web, files disguised as a legitimate CMS plugin, and files with an e-mail transmission function.

To perform such defacements or plant such files, the attackers could have cracked an FTP or SSH password to gain access to the server, uploaded the files using a vulnerability, cracked the password to the administration screen of a CMS, uploaded a malicious file disguised as a plugin via remote control, or used any other method.

Countermeasures include performing the following on the server's administration screen or on the FTP or SSH server: restricting access only from specific IP addresses, setting a sufficiently long password that is hard to guess, keeping CMS, themes and plugins up to date, and completely removing unnecessary themes and plugins from the system instead of just disabling them.

[Defacement of e-commerce websites using Magento]

Around the end of November, JPCERT/CC was notified by the CERT Nazionale Italia of Italy that a number of e-commerce websites built using a CMS called Magento were embedded with a code designed to steal credit card information and credentials. JPCERT/CC investigated each domestic e-commerce websites on the list of affected websites that was provided. As a result, it was found that a suspicious script was embedded in the top page on a number of the websites, and, on other websites, in the JavaScript code for checking if credit card numbers are entered correctly.

JPCERT/CC requested a number of hosting providers that administer the e-commerce websites embedded with a suspicious script to check and confirm whether the code was intended.

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

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.

About the Mailing List
https://www.jpcert.or.jp/announce.html

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 2016Fiscal Year".

JPCERT Coordination Center (JPCERT/CC)
https://www.jpcert.or.jp/