JPCERT Coordination Center

JPCERT/CC Incident Handling Report

April 1, 2024 - June 30, 2024

JPCERT Coordination Center

July 18, 2024

JPCERT CC®

Table of Contents

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 2024 Fiscal Year".

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 incident reports received during the period from April 1, 2024 through June 30, 2024, from both quantitative and qualitative perspectives using statistics and case examples.

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

[Chart 2.1 Number of incident reports]

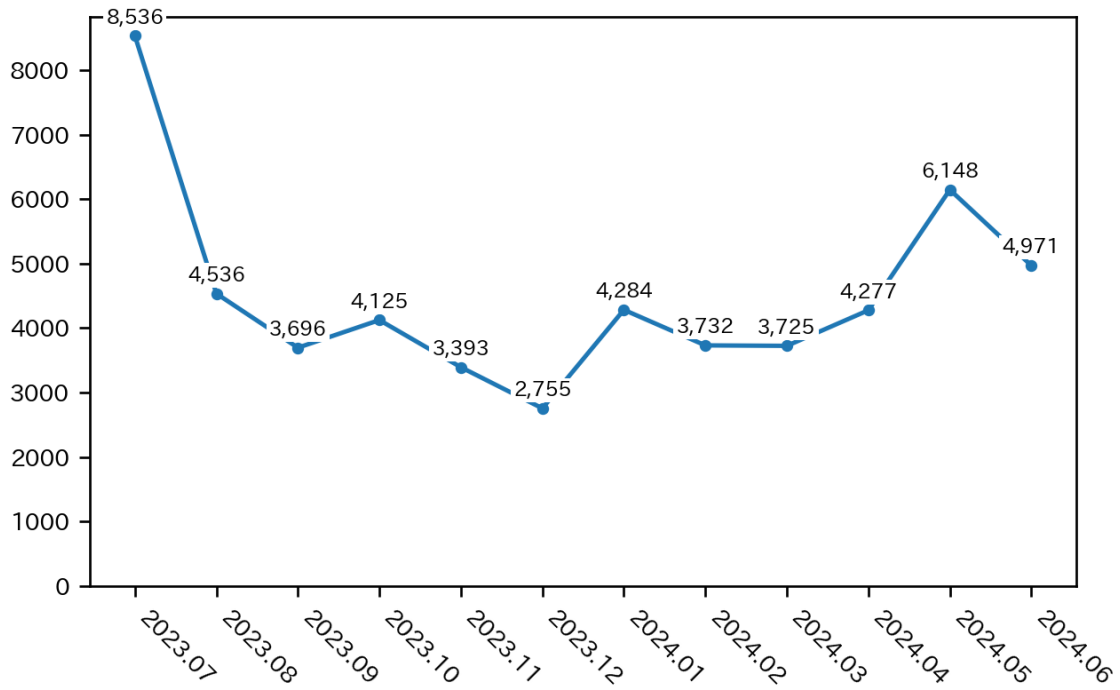
	Apr	May	Jun	Total	Last Qtr. Total
Number of Reports [(2)]	4,277	6,148	4,971	15,396	11,741
Number of Incident [(3)]	2,280	2,398	1,926	6,604	6,089
Cases Coordinated [(4)]	1,541	1,375	1,260	4,176	4,602

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

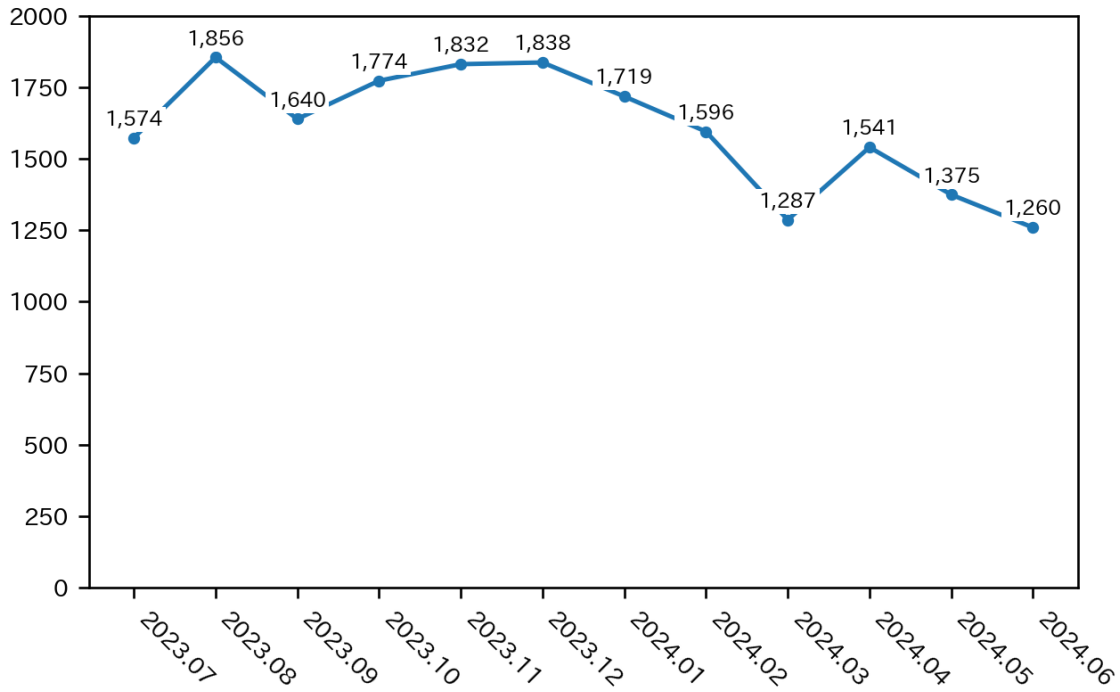
(3) "Number of Incidents" refers to the number of incidents contained in each report. Multiple reports on the same incidents are counted as 1 incident.

(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 15,396. Of these, the number of cases that JPCERT/CC coordinated was 4,176. When compared with the previous quarter, the number of reports increased by 31%, and the number of cases coordinated decreased by 9%. Year on year, the number of reports decreased by 43%, and the number of cases coordinated decreased by 9%.
[Figure 2.1] and [Figure 2.2] show the monthly changes in the total number of reports and incident cases coordinated by JPCERT/CC over the past fiscal year.



[Figure 2.1 Change in the number of incident reports]

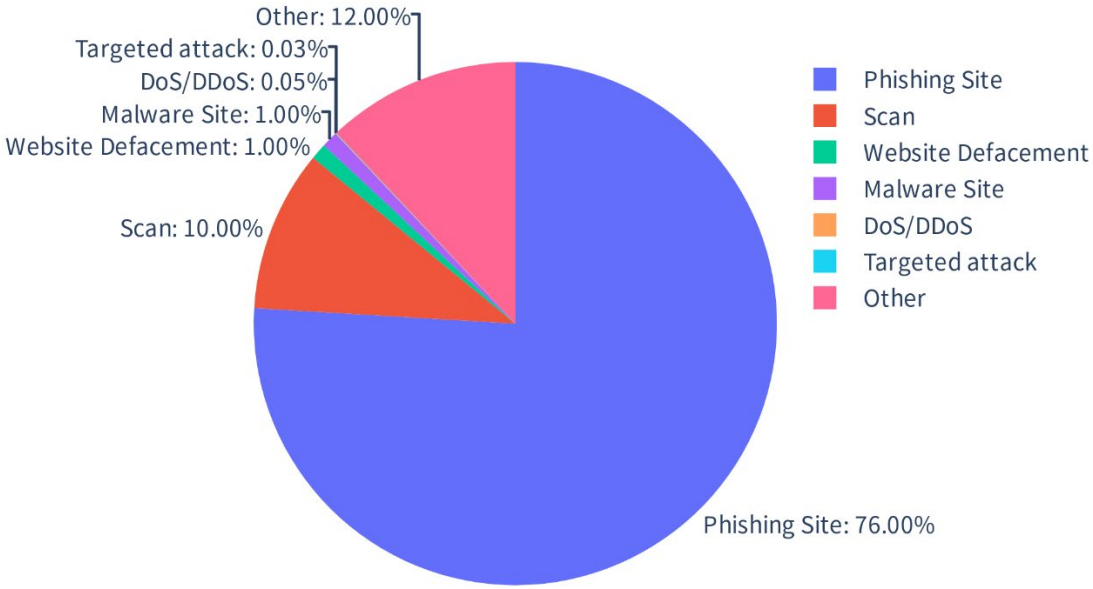


[Figure 2.2 Change in the number of incident cases coordinated]

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 2.2] shows a breakdown of the number of incidents reported during the quarter by category. A breakdown of the percentage is shown in [Figure 2.3].

[Chart 2.2 Number of incident reports by category]

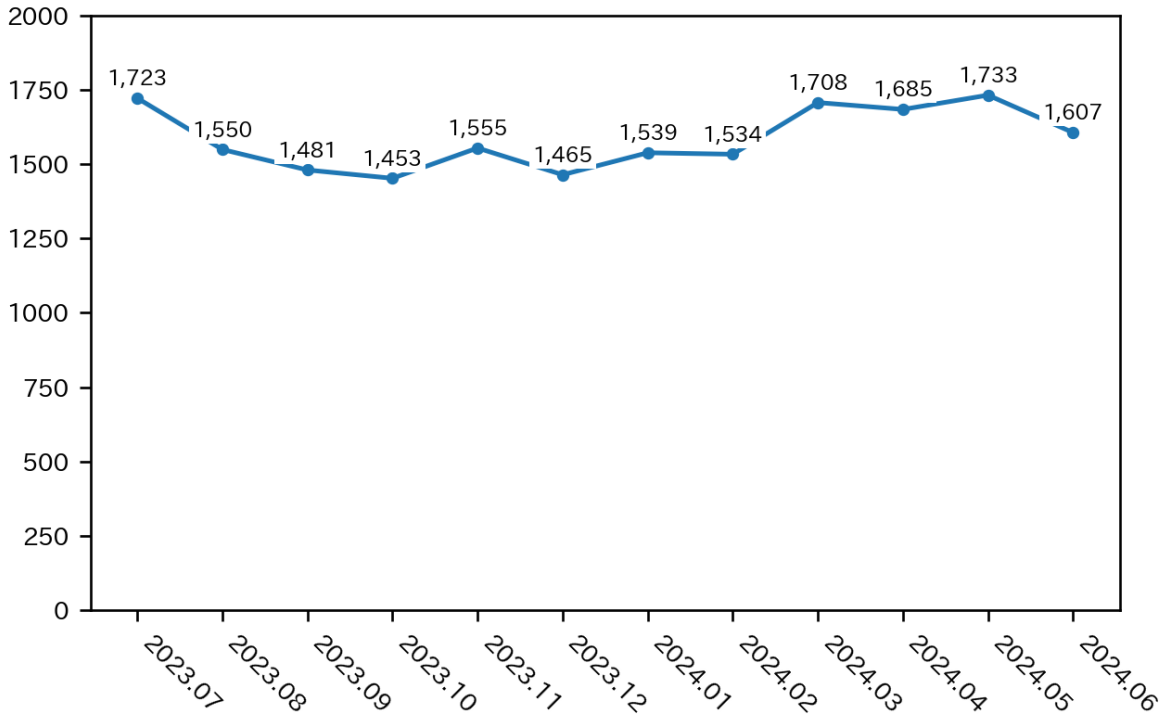
Incident Category	Apr	May	Jun	Total	Last Qtr.Total
Phishing Site	1,685	1,733	1,607	5,025	4,781
Website Defacement	8	20	15	43	57
Malware Site	28	12	5	45	45
Scan	252	285	152	689	697
DoS/DDoS	0	1	2	3	2
ICS Related	0	0	0	0	0
Targeted attack	2	0	0	2	4
Other	305	347	145	797	503



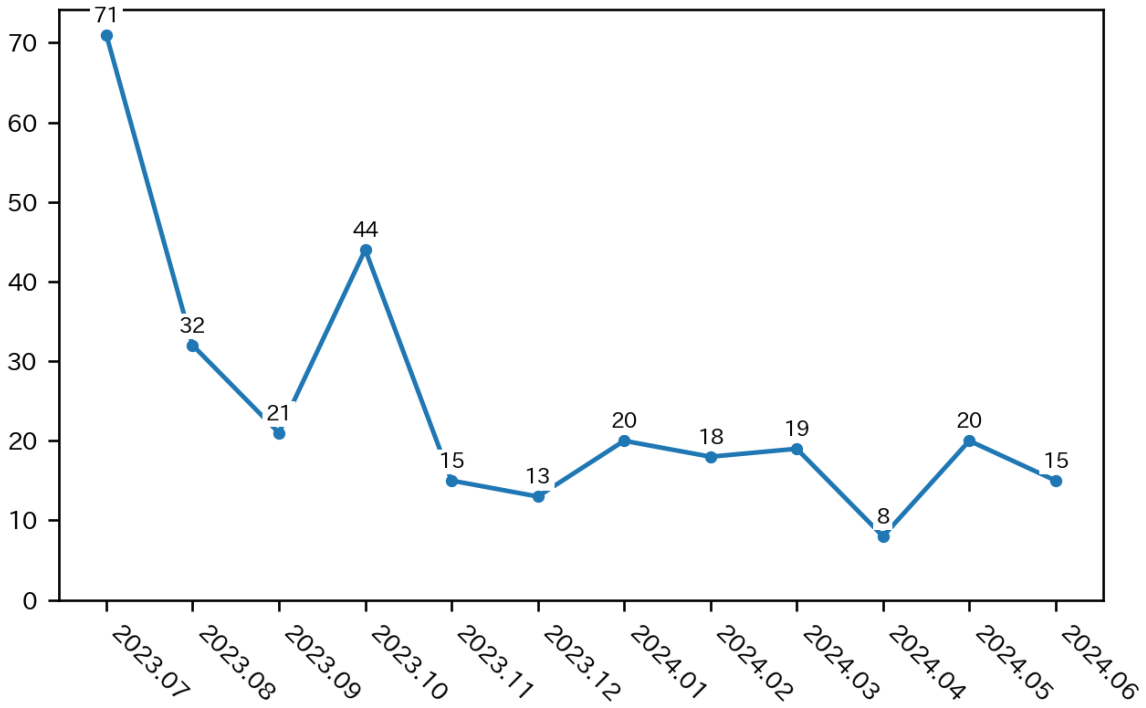
[Figure 2.3 Percentage of incidents by category]

Incidents categorized as phishing sites accounted for 76%, and those categorized as scans, which search for vulnerabilities in systems, made up 10%.

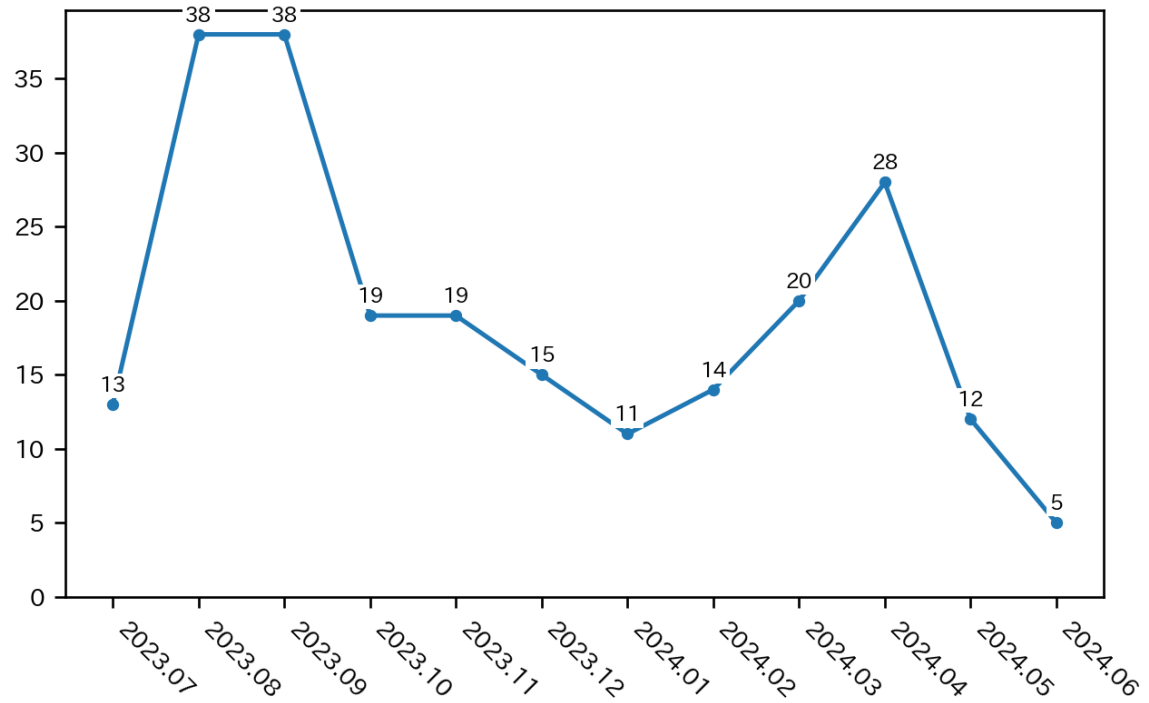
[Figure 2.4] through [Figure 2.7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



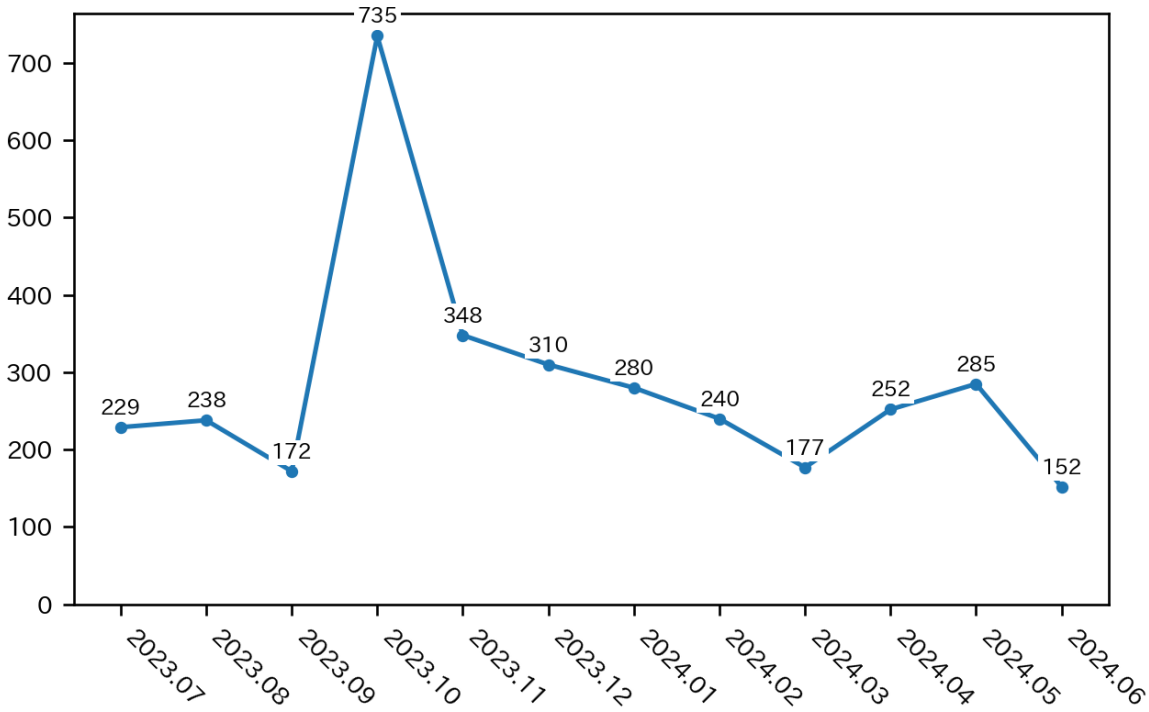
[Figure 2.4 Change in the number of phishing sites]



[Figure 2.5 Change in the number of website defacements]

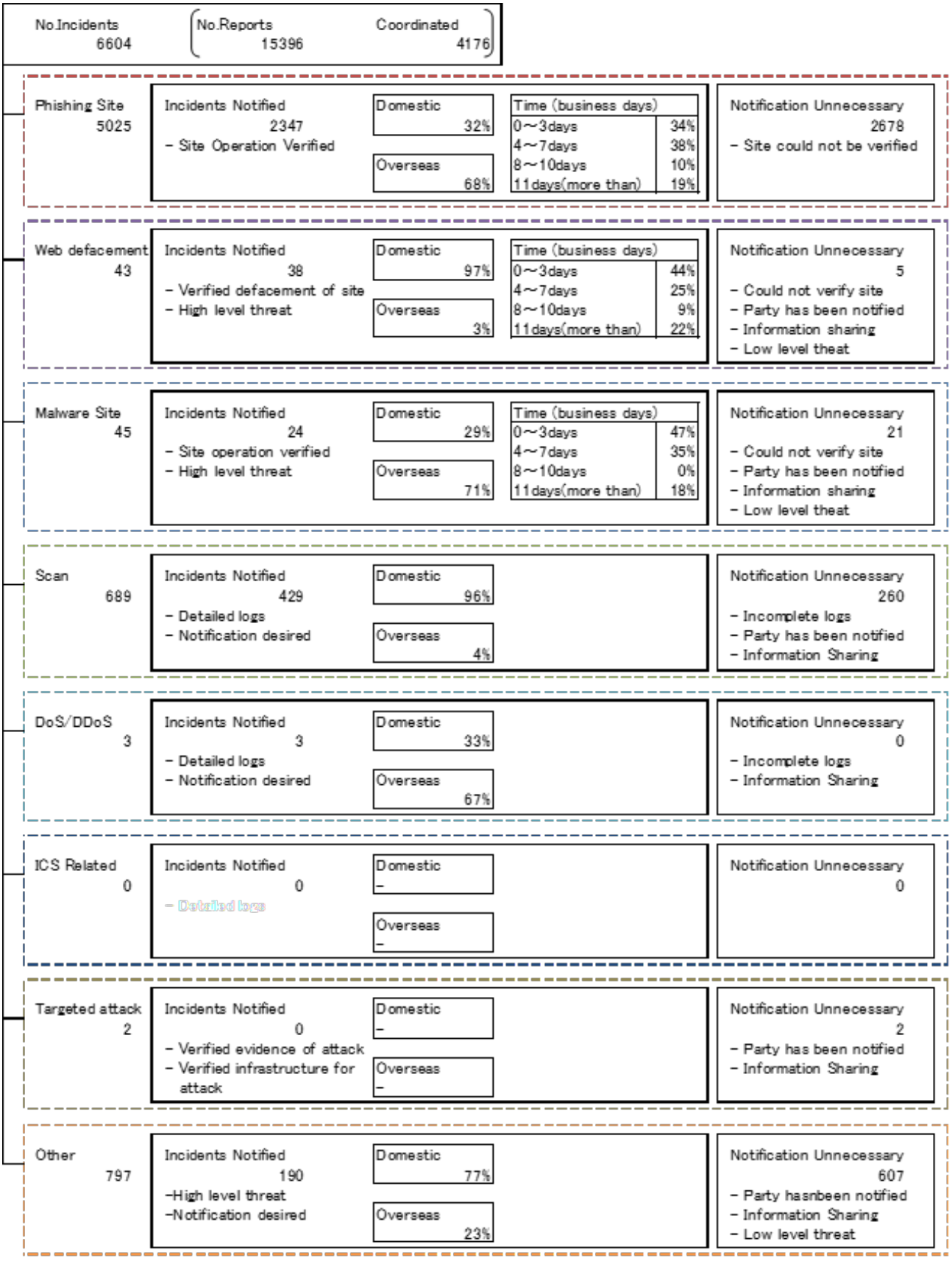


[Figure 2.6 Change in the number of malware sites]



[Figure 2.7 Change in the number of scans]

[Figure 2.8] provides an overview as well as a breakdown of the incidents that were coordinated /Handled.



[Figure 2.8 Breakdown of incidents coordinated/handled]

3. Incident Trends

3.1. Phishing Site Trends

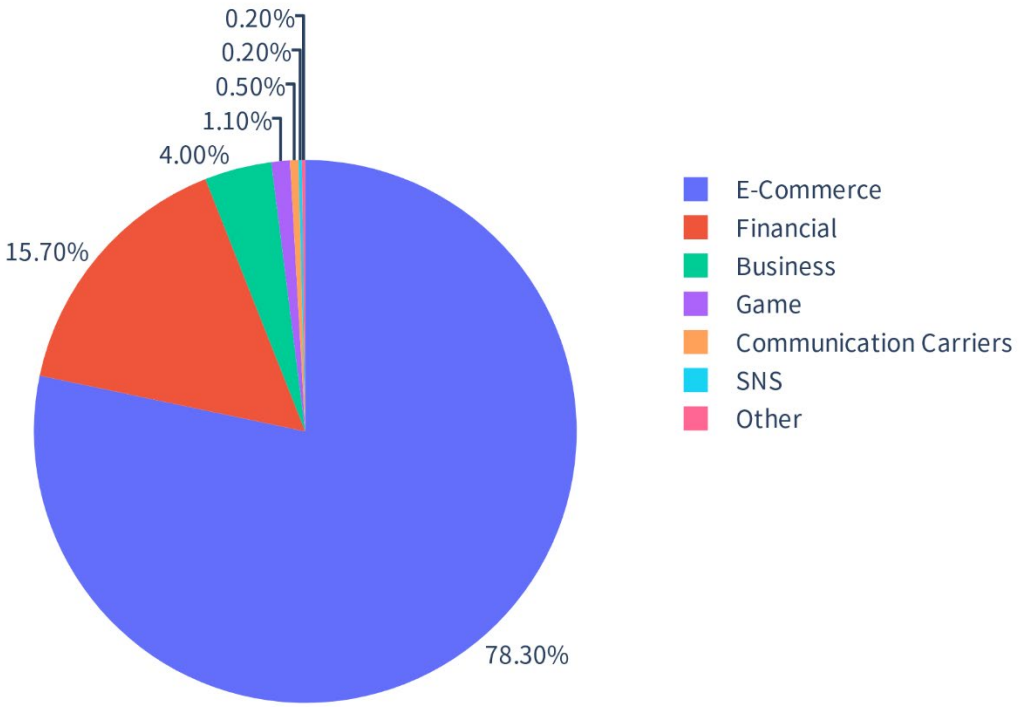
During this quarter, 5,025 reports on phishing sites were received, representing a 5% increase from 4,781in the previous quarter. This marks a 19% decrease from the same quarter last year (6,186).

During this quarter, there were 961 phishing sites that spoofed overseas brands, increasing 29% from 745 in the previous quarter. There were 3,026 phishing sites that spoofed domestic brands, decreasing 6% from 3226 in the previous quarter. The numbers of phishing sites reported in this quarter for overseas and domestic brands are shown in [Chart 3.1]. The percentages of phishing sites reported in this quarter by industry for overseas and domestic brands are shown in [Figure 3.1] [Figure 3.2].

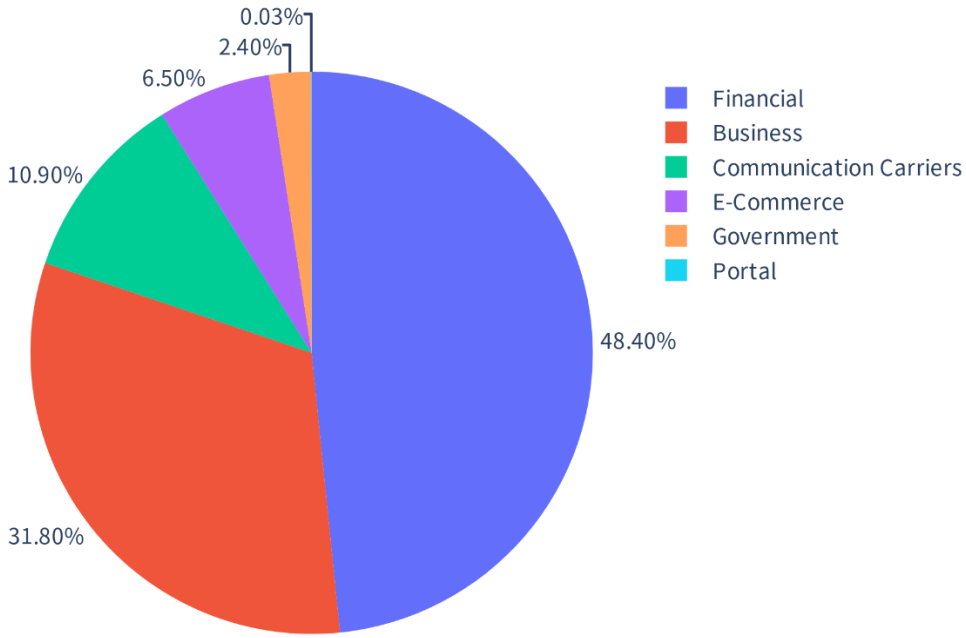
[Chart 3.1 Number of phishing sites for domestic and overseas brands]

Phishing Site	Apr	May	Jun	Domestic/Overseas Total (%)
Domestic Brand	1,101	1,048	877	3,026 (60%)
Overseas Brand	293	336	332	961 (19%)
Unknown Brand (5)	291	349	398	1,038 (21%)
Monthly Total	1,685	1,733	1,607	5,025

(5) "Unknown Brand" refers to sites which could not be verified since the reported site had already been suspended when accessed for confirmation.



[Figure 3.1 Percentage of reported phishing sites by industry for overseas brands]



[Figure 3.2 Percentage of reported phishing sites by industry for domestic brands]

Out of the total number of phishing sites reported to JPCERT/CC, 78% spoofed e-commerce websites for overseas brands and 48% spoofed financial websites for domestic brands, both representing the largest share respectively.

For overseas brands, phishing sites spoofing Amazon and Apple accounted for more than 80% of the phishing sites reported.
For domestic brands, phishing sites spoofing Mercari and Eki-Net were reported in large numbers. Among domestic financial institutions, phishing sites spoofing EPOS Card, Aeon Card, and Sumitomo Mitsui Card continued to be seen in large numbers as in the previous quarter.

The websites that JPCERT/CC coordinated with to take down phishing sites were 32% domestic and 68% overseas for this quarter, indicating an increase in domestic parties compared to the previous quarter (domestic: 30%, overseas: 70%).

3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 43. This was a 25% decrease from 57 in the previous quarter.

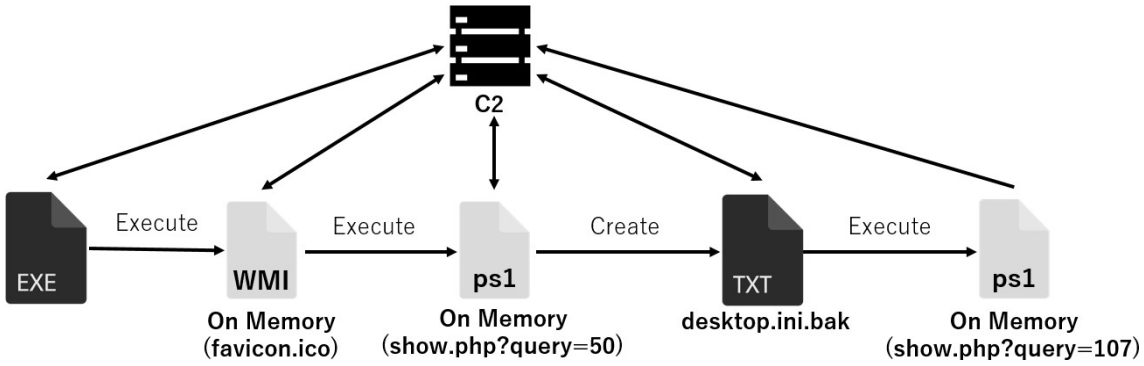
During this quarter, JPCERT/CC confirmed cases of redirection to suspicious websites exploiting the browser's notification function. Legitimate websites were planted with malicious PHP code, which used the browser's notification function to redirect users who accessed them to suspicious websites. Also, the

malicious PHP code sent a DNS query to a domain provided by the attackers, and the data included in the TXT record of the response was used as the URL to which users were redirected. To insert the malicious PHP code into legitimate websites, the attackers had installed a plugin called WPCode in the compromised websites.

3.3. Targeted Attack Trends

There were 2 incidents categorized as a targeted attack.

This quarter, JPCERT/CC received reports of targeted attack e-mails. The file attached to targeted attack e-mails had numerous spaces before the .exe extension to make it difficult to identify the file type. When the attached file is executed, malware that sends system information and keyboard entry data to a C2 server gets downloaded. The downloaded malware is written with PowerShell, and it is run on memory without being saved as a file on the hard drive. [[Figure 3.3] shows the flow of events up to infection with malware.



[Figure 3.3 Flow of events from execution of attached file to malware infection]

3.4. Other Incident Trends

The number of malware sites reported in this quarter was 45, which remained unchanged from the previous quarter.
The number of scans reported in this quarter was 689. This was a 1% decrease from 697 in the previous quarter. The top 10 ports that the scans targeted are listed in [Chart3.2]. Ports targeted frequently were Telnet (23/TCP),SSH (22/TCP),SMTP (25/TCP) and HTTPS(443/TCP).

[Chart 3.2 Top 10 ports by number of scans]

Port	Apr	May	Jun	Total
23/tcp	106	117	122	345
22/tcp	90	64	19	173
25/tcp	29	52	7	88
443/tcp	10	34	2	46
80/tcp	13	9	2	24
37215/tcp	3	2	0	5
2323/tcp	1	2	0	3
143/tcp	1	2	0	3
110/tcp	1	1	0	2
9530/tcp	1	0	0	1

There were 797 incidents categorized as other. This was a 58% increase from 503 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 PAN-OS GlobalProtect vulnerabilities

On April 12, 2024, Palo Alto Networks announced that the GlobalProtect feature of PAN-OS had an OS command injection vulnerability (CVE-2024-3400). GlobalProtect is a feature that provides remote access (VPN), and by exploiting this vulnerability, an unauthenticated third party may remotely execute any code with administrative access. As this vulnerability was already exploited in the wild, JPCERT/CC also issued a security alert on April 13.

Security alert concerning OS command injection vulnerability (CVE-2024-3400) in GlobalProtect of Palo Alto Networks PAN-OS (Japanese only)
https://www.jpcert.or.jp/at/2024/at240009.html

JPCERT/CC received reports of damage due to this vulnerability from a number of organizations. Many of the incidents occurred after the vulnerability was announced and a patch was released on April 14. The configuration file of the affected device was copied to a place which is publicly accessible, and its content was leaked. Organizations that had disabled device telemetry, which is a workaround for the vulnerability, were able to prevent attacks.
Based on information provided by external organizations, JPCERT/CC alerted system administrators in Japan who were using devices that could have been compromised due to exploitation of this vulnerability. As of April 20, there were 252 potentially compromised devices in Japan. All the organizations have been alerted, and as of June 11 this number has decreased to 86. Many of the organizations were not aware of the infringement until they were alerted, and some of them even failed to notice that the content altered by the attacker had been automatically corrected by the threat defense feature of the device. When a vulnerability with confirmed cases of exploitation is announced, it is advisable to check for any infringement before updating the device.

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.)

For the latest information, please refer to JPCERT/ CC's website.

- JPCERT Coordination Center (JPCERT/CC)
  https://www.jpcert.or.jp/english/
- Sharing incident information and requesting
  coordinationinfo@jpcert.or.jp, https://www.jpcert.or.jp/form/
- Inquiries about vulnerability information handling
  vultures@jpcert.or.jp
- Inquiries about ICS security
  icsr@jpcert.or.jp
- Inquiries about secure coding seminars
  secure-coding@jpcert.or.jp
- Inquiries about citing published documents, requesting a presentation, etc.
  pr@jpcert.or.jp
- PGP public keys
  https://www.jpcert.or.jp/jpcert-pgp.html

JPCERT/CC Incident Handling Report [April 1, 2024 - June 30, 2024]

- First version issued: September 5, 2024
- Issued by:
  Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)
  8F Tozan Bldg, 4-4-2 Nihonbashi-Honcho, Chuo-ku, Tokyo 103-0023, Japan