JPCERT/CC Incident Handling Report

July 1, 2024 - September 30, 2024

JPCERT Coordination Center

October 17, 2024

JPCERT CC®

Table of Contents

1. About the Incident Handling Report 3
2. Quarterly Statistics 4
3. Incident Trends 10
3.1. Phishing Site Trends 10
3.2. Website Defacement Trends 11
3.3. Targeted Attack Trends 12
3.3.1. Targeted attack e-mails exploiting Google Drive 12
3.3.2. Targeted attack e-mails causing ANEL malware infections 12
3.4. Other Incident Trends 13
4. Incident Handling Case Examples 14
4.1. Coordination involving cases of SSL-VPN vulnerabilities being exploited to steal credentials 14
Request from JPCERT/CC 15
Appendix-1. Classification of Incidents 16

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 July 1, 2024 through September 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]

	Jul	Aug	Sep	Total	Last Qtr. Total
Number of Reports (2)	4,627	3,095	3,075	10,797	15,396
Number of Incident (3)	1,821	1,779	1,547	5,147	6,604
Cases Coordinated (4)	1,071	1,167	1,093	3,331	4,176

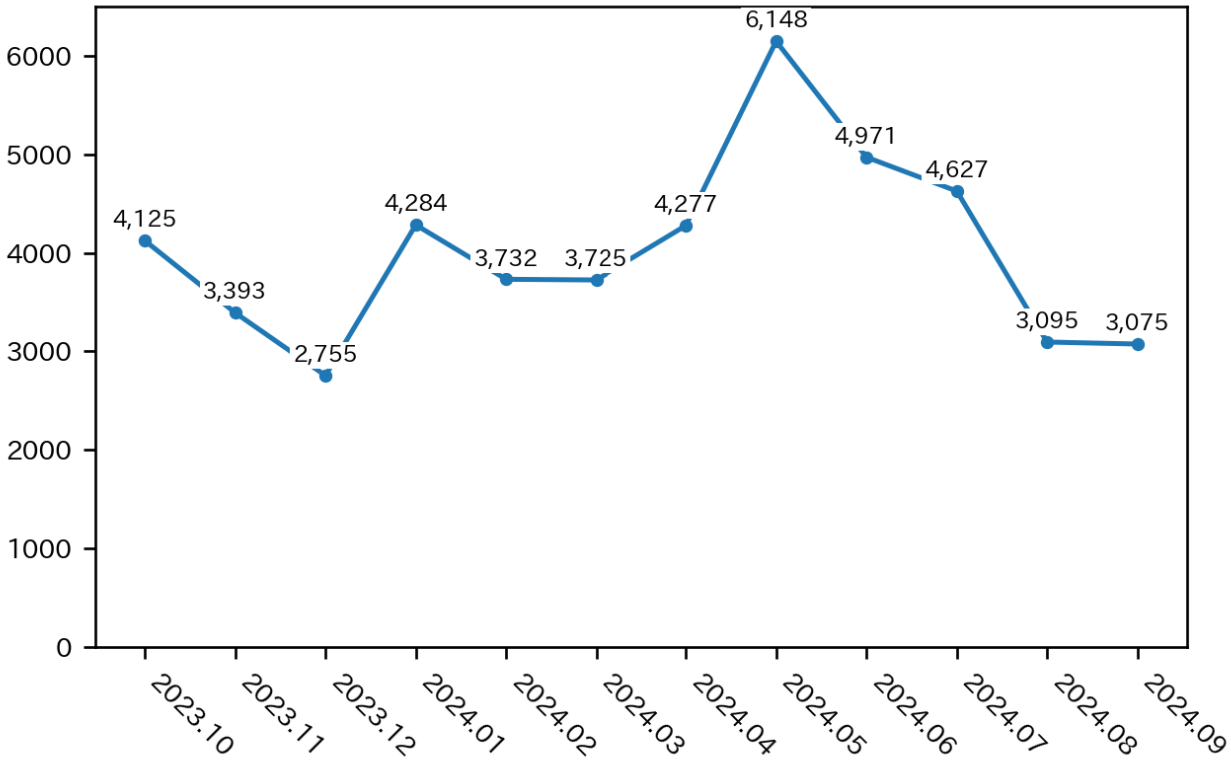
(2) "Number of Reports" refers to the total number of reports sent through the web form, e-mail or FAX.

(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.

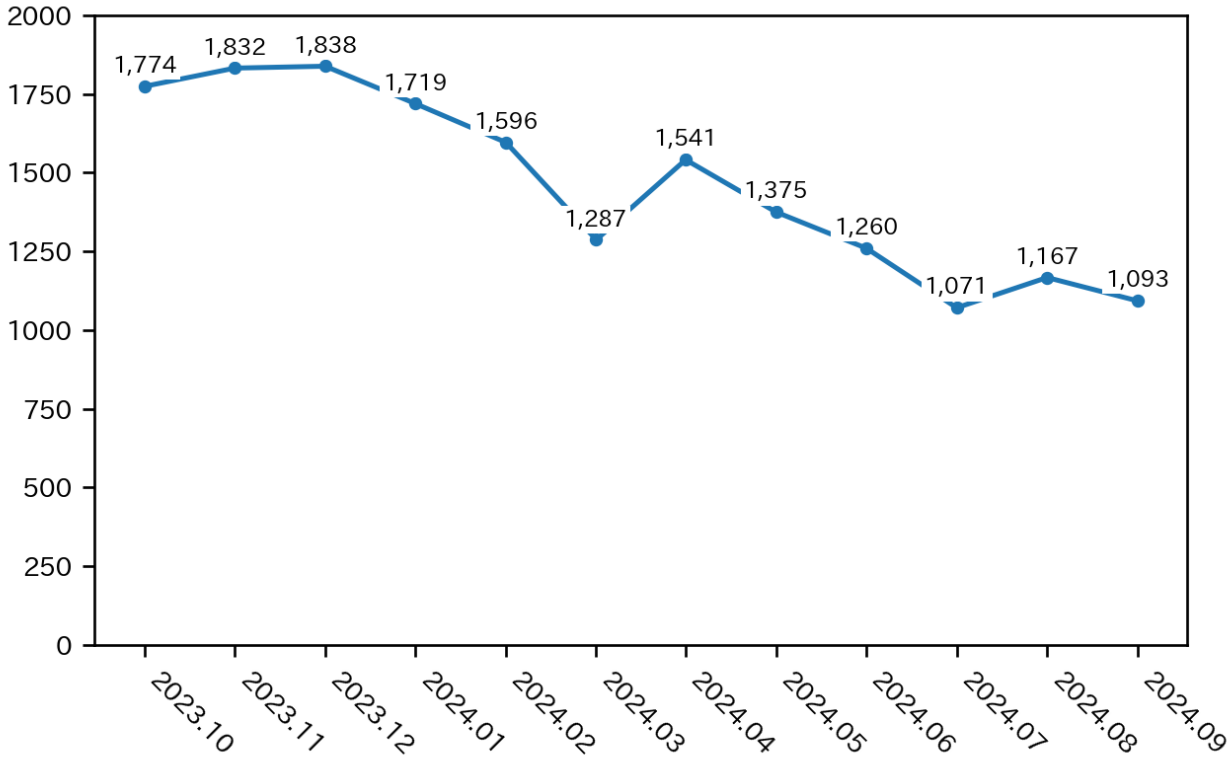
(4) "Number of Cases Coordinated" refers to the number of cases where coordination took place to prevent the spreading of an incident by sending them a report and asking the site administrator to address any issues.

The total number of reports received in this quarter was 10,797. Of these, the number of cases that JPCERT/CC coordinated was 3,331. When compared with the previous quarter, the number of reports decreased by 30%, and the number of cases coordinated decreased by 20%. Year on year(16,768 reports received, 5,070 cases coordinated), the number of reports decreased by 36%, and the number of cases coordinated decreased by 34%.

[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]

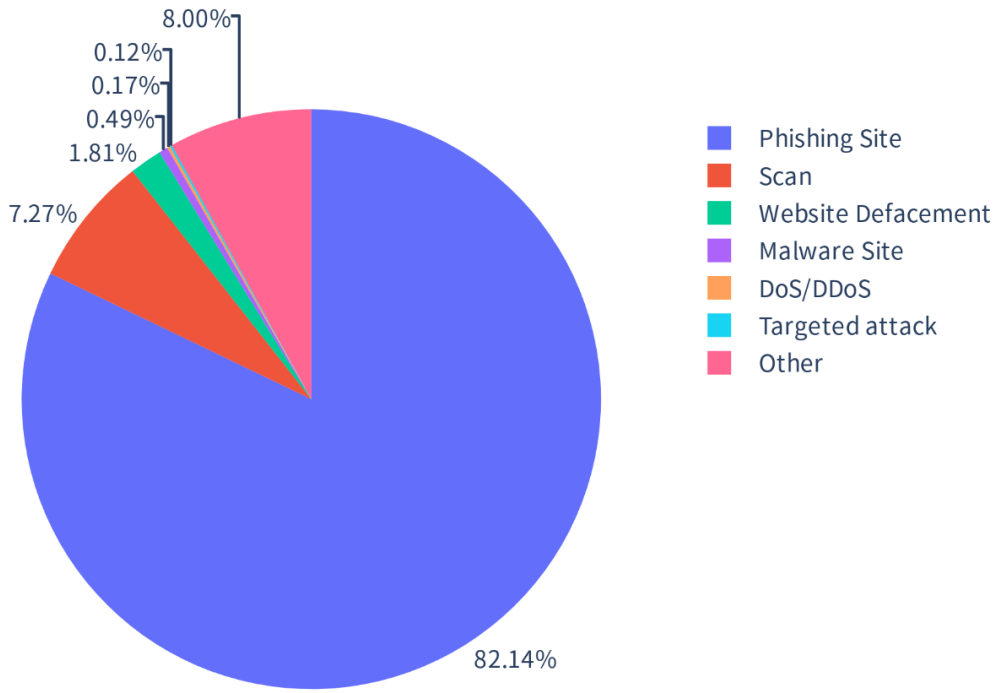


[Figure 2.2 Change in the number of incident cases coordinated]

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]

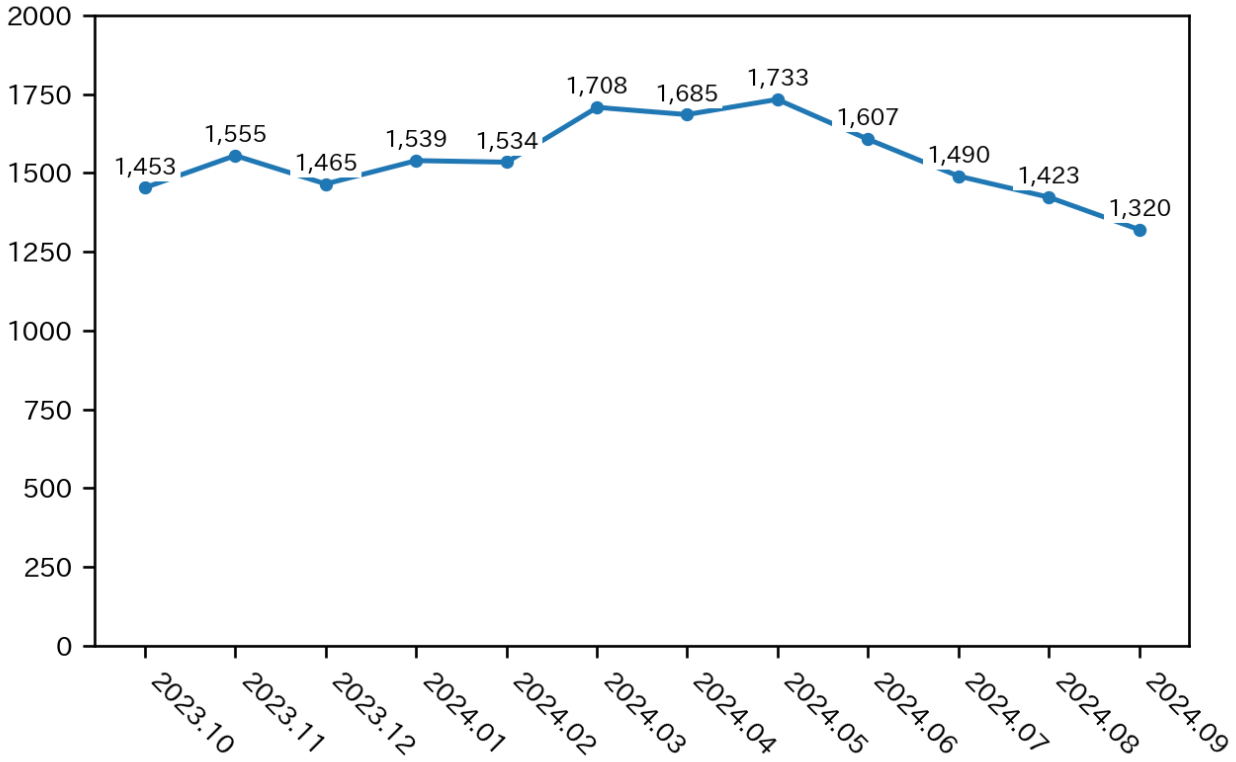
Incident Category	Jul	Aug	Sep	Total	Last Qtr.Total
Phishing Site	1,490	1,423	1,320	4,233	5,025
Website Defacement	61	25	7	93	43
Malware Site	9	10	6	25	45
Scan	154	127	93	374	689
DoS/DDoS	0	5	4	9	3
ICS Related	0	0	0	0	0
Targeted attack	0	1	5	6	2
Other	107	188	112	407	797



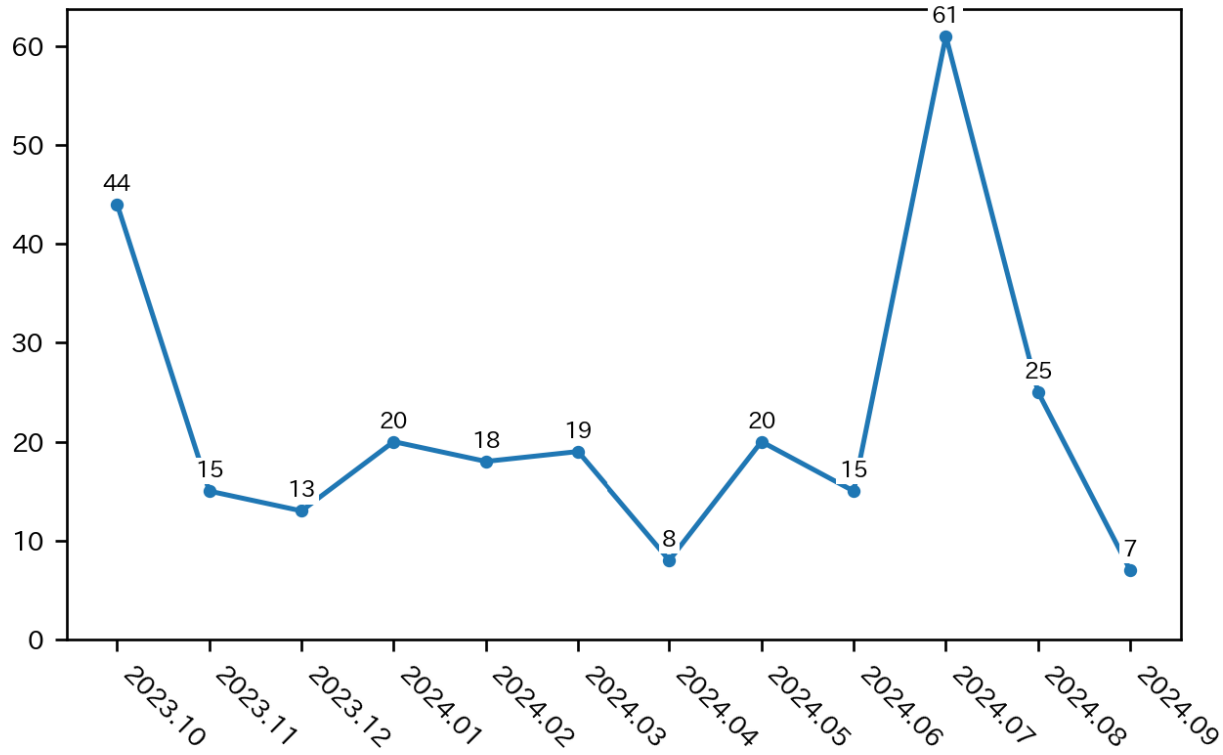
[Figure 2.3 Percentage of incidents by category]

Incidents categorized as phishing sites accounted for 82%, and those categorized as scans, which search for vulnerabilities in systems, made up 7%.

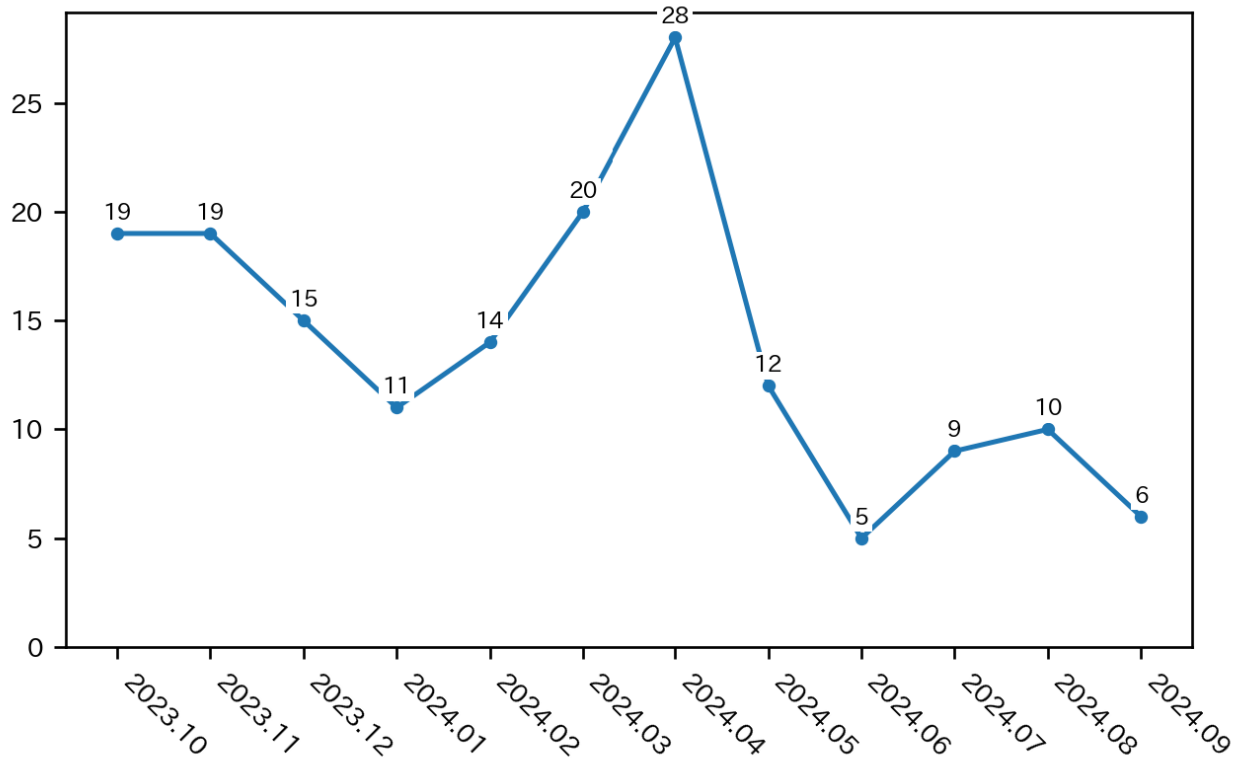
[Figure 2.4] through [Figure 2.7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



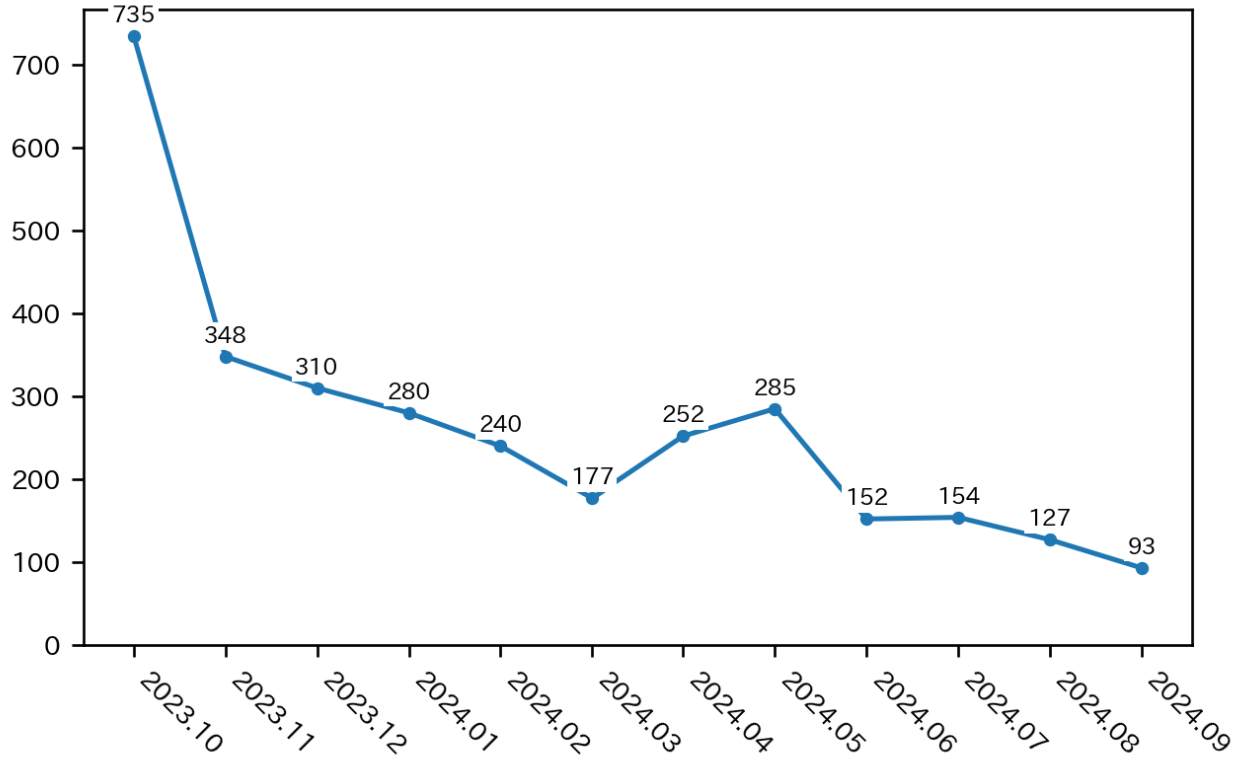
[Figure 2.4 Change in the number of phishing sites]



[Figure 2.5 Change in the number of website defacements]

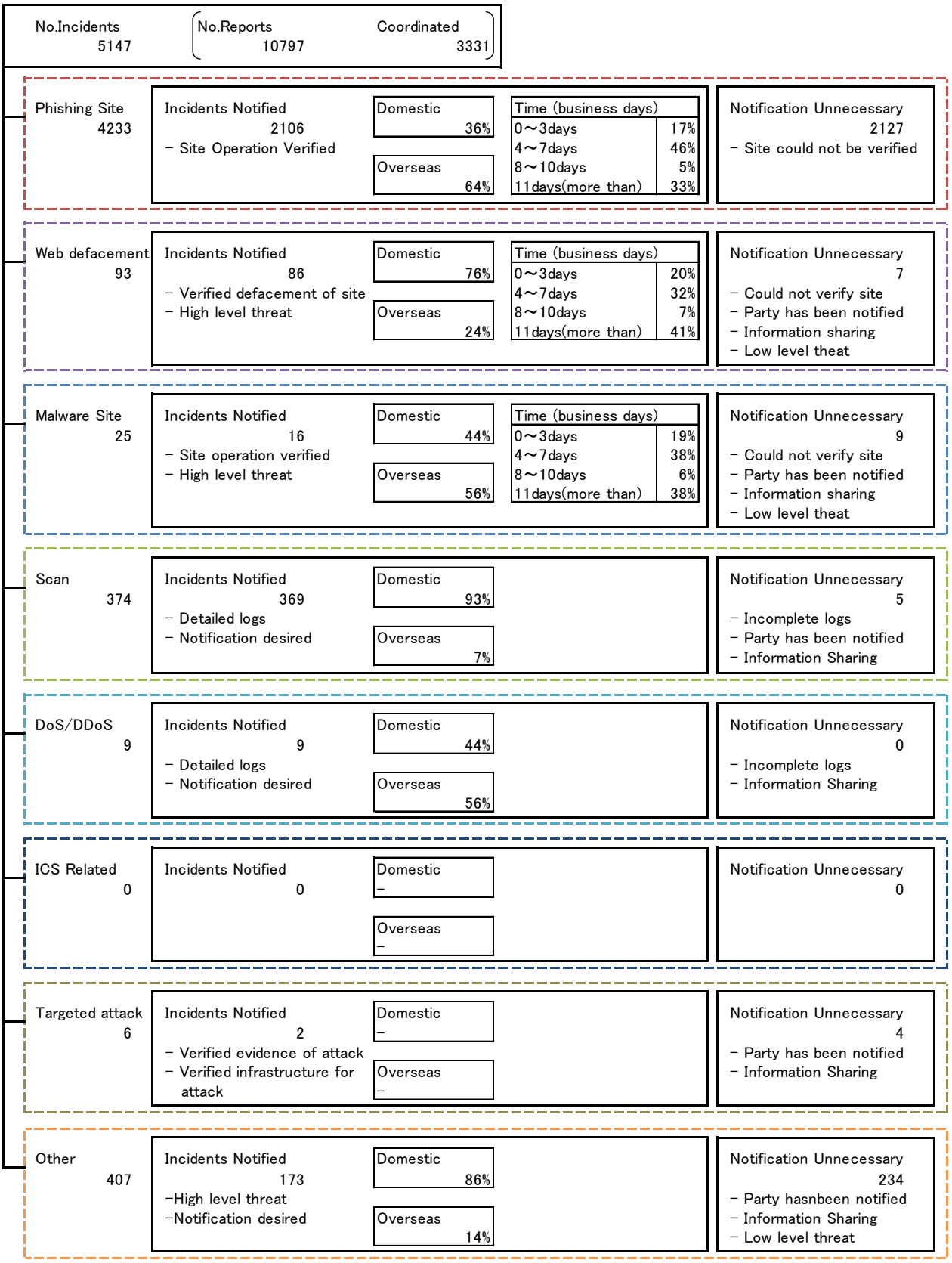


[Figure 2.6 Change in the number of malware sites]



[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

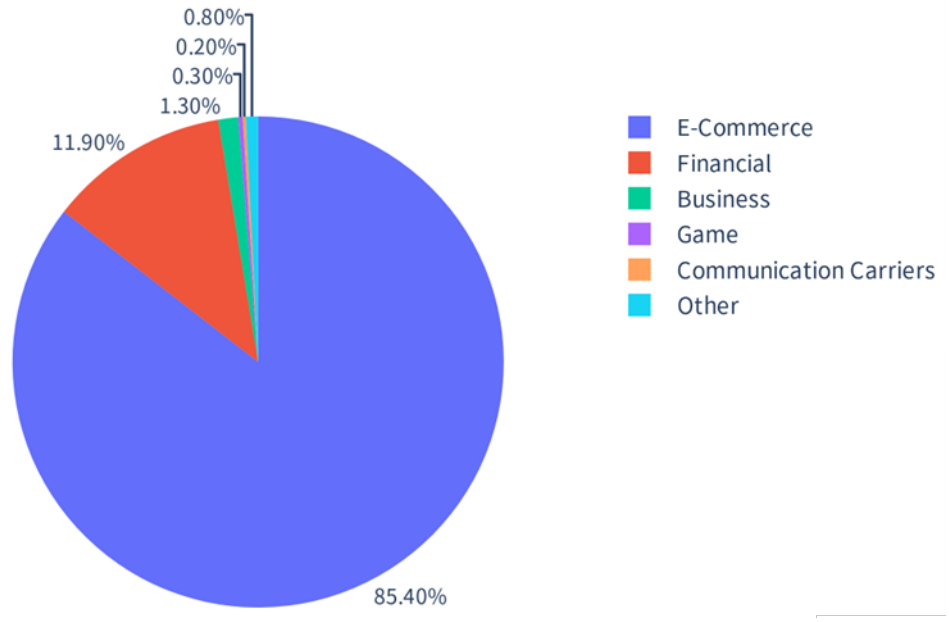
During this quarter, 4,233 reports on phishing sites were received, representing a 16% decrease from 5,025 in the previous quarter. This marks a 11% decrease from the same quarter last year (4,754).

During this quarter, there were 597 phishing sites that spoofed overseas brands, decreasing 38% from 961 in the previous quarter. There were 2,883 phishing sites that spoofed domestic brands, decreasing 5% from 3,026 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].

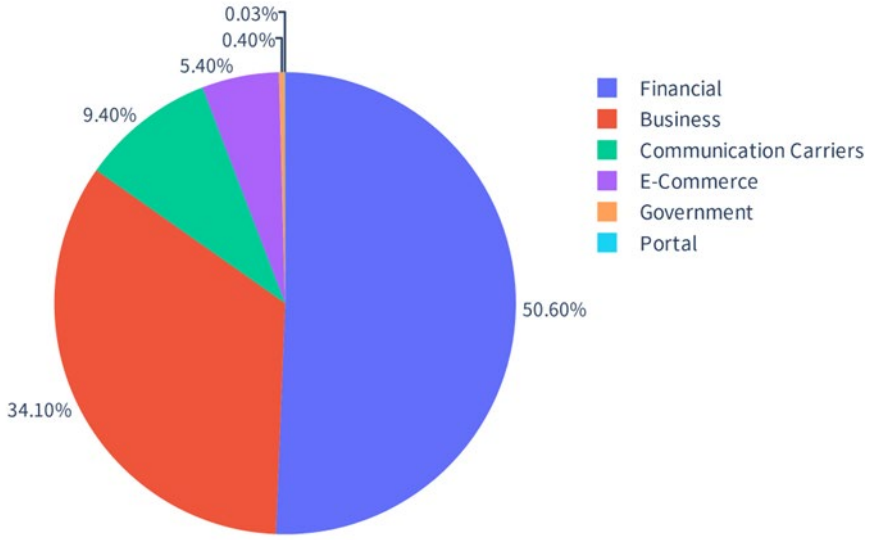
[Chart 3.1 Number of phishing sites for domestic and overseas brands]

Phishing Site	Jul	Aug	Sep	Domestic/Overseas Total (%)
Domestic Brand	859	998	1,026	2,883 (68%)
Overseas Brand	250	204	143	597 (14%)
Unknown Brand (5)	381	221	151	753 (18%)
Monthly Total	1,490	1,423	1,320	4,233

(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, 85% spoofed e-commerce websites for overseas brands and 51% spoofed financial websites for domestic brands, both representing the largest share respectively.

For overseas brands, phishing sites spoofing Amazon accounted for around 90% of the phishing sites reported.
For domestic brands, phishing sites spoofing Eki-Net and Yamato Transport were reported in large numbers. Among domestic financial institutions, phishing sites spoofing Aeon Card, Sumitomo Mitsui Card and JCB 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 36% domestic and 64% overseas for this quarter, indicating an increase in domestic parties compared to the previous quarter (domestic: 32%, overseas: 68%).

3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 93. This was a 116% increase from 43 in the previous quarter.

This quarter, the following types of website defacements were reported in large numbers.
1. Website defacements intended to redirect users who accessed the website to a fake e-commerce site
2. Placement of a suspicious JavaScript file that lures users who accessed the website to download malware
3. Placement of a JavaScript file aimed at stealing data entered by users who accessed the website

The third type of defacement included the placement of a JavaScript file that encodes the data users enter on the website to Base64 format and sends it to a suspicious external server.

3.3. Targeted Attack Trends

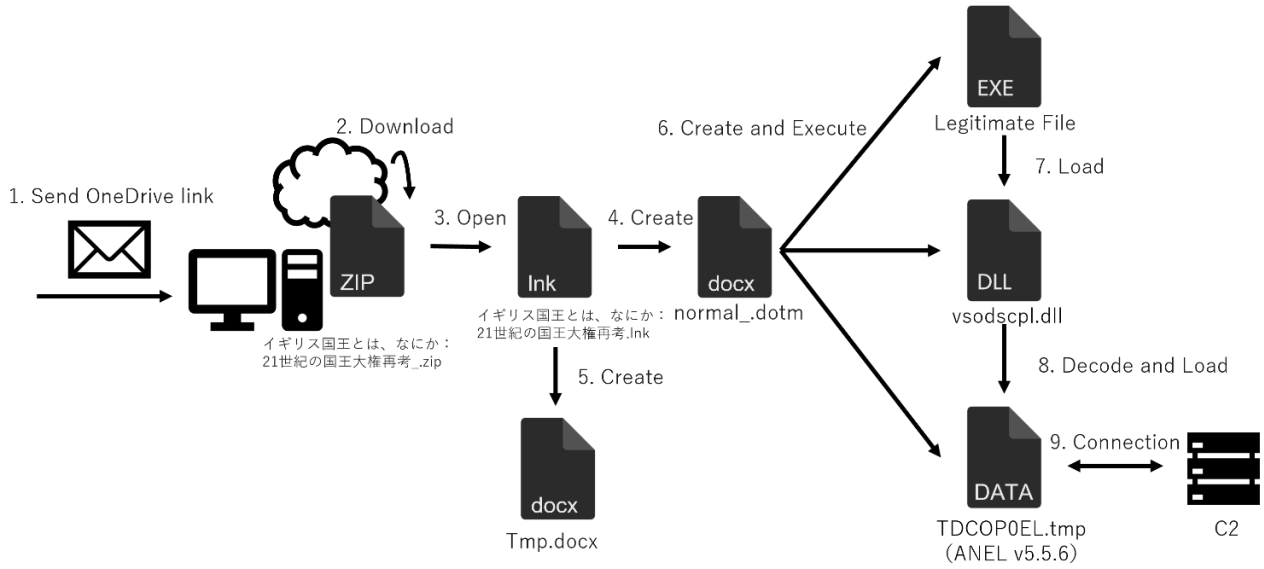
There were 6 incidents categorized as a targeted attack. This quarter, JPCERT/CC received a number of reports of targeted attack e-mails.

3.3.1. Targeted attack e-mails exploiting Google Drive

During this quarter, there were a number of reports concerning targeted attack e-mails exploiting Google Drive. The targeted attack e-mails that were reported contained a Google Drive link for sharing a file, which was a virtual hard disk (VHDX) file. When the shared file is downloaded and the LNK file inside is executed, malware is downloaded and infects the computer. Judging from the characteristics of the downloaded malware, a group known as "APT-C-60" is presumably behind this attack.

3.3.2. Targeted attack e-mails causing ANEL malware infections

This quarter, JPCERT/CC confirmed that targeted attack e-mails attempting to cause infection with the ANEL malware were sent to a number of organizations. The e-mail had "What is the British Monarch?: Rethinking the Royal Prerogative in the 21st Century" as the subject (in Japanese) and contained a link for a file-sharing service that downloads a ZIP file. The ZIP file contained an LNK file that, when executed, runs a Word macro placed inside, infecting the computer with malware. [Figure 3.3] shows the flow of events up to infection with malware.



[Figure 3.3 Flow of events up to infection with ANEL malware]

3.4. Other Incident Trends

The number of malware sites reported in this quarter was 25. This was a 44% decrease from 45 in the previous quarter.
The number of scans reported in this quarter was 374. This was a 46% decrease from 689 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), 37215/TCP and 8080/TCP.

[Chart 3.2 Top 10 ports by number of scans]

Port	Jul	Aug	Sep	Total
23/tcp	123	91	63	277
22/tcp	14	18	13	45
37215/tcp	3	5	3	11
8080/tcp	2	2	6	10
443/tcp	1	1	6	8
9530/tcp	1	5	1	7
8888/tcp	3	0	1	4
2323/tcp	1	1	2	4
52869/tcp	1	2	0	3
80/tcp	1	1	0	2

There were 407 incidents categorized as others. This was a 49% decrease from 797 in the previous quarter.

4. Incident Handling Case Examples

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

4.1. Coordination involving cases of SSL-VPN vulnerabilities being exploited to steal credentials

There have been ongoing cases in which vulnerabilities in SSL-VPN have presumably been exploited to steal credentials, and a number of such cases were reported again this quarter. CVE-2023-27997 and CVE-2024-21762 are presumed to be among the exploited vulnerabilities. In some of the cases, the products already had a fix (patch) applied to address the vulnerabilities at the time of intrusion, but the attacker used credentials they had stolen before the fix was applied to gain access to the network.
When a vulnerability with confirmed cases of exploitation is announced, it is advisable to check for any signs of intrusion into the relevant device before updating its firmware. If the possibility of intrusion cannot be denied, it may be necessary to consider the possibility that credentials have been stolen and to change the passwords of the accounts that were being used.

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 [July 1, 2024 - September 30, 2024]

- First version issued: December 6, 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