JPCERT/CC Incident Handling Report

January 1, 2025 - March 31, 2025

JPCERT Coordination Center

April 17, 2025

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 January 1, 2025 through March 31, 2025, 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.

The total number of reports received in this quarter was 10,102. Of these, the number of cases that JPCERT/CC coordinated was 3,974. When compared with the previous quarter, the number of reports increased by 4%, and the number of cases coordinated increased by 10%. Year on year (11,741 reports received, 4,602 cases coordinated), both the number of reports and number of cases coordinated decreased by 14%.

[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.

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 2.1 Number of incident reports]

	Jan	Feb	Mar	Total	Last Qtr. Total
Number of Reports (2)	3,294	2,840	3,968	10,102	9,743
Number of Incident (3)	1,919	2,014	2,148	6,081	5,561
Cases Coordinated (4)	1,380	1,377	1,217	3,974	3,597

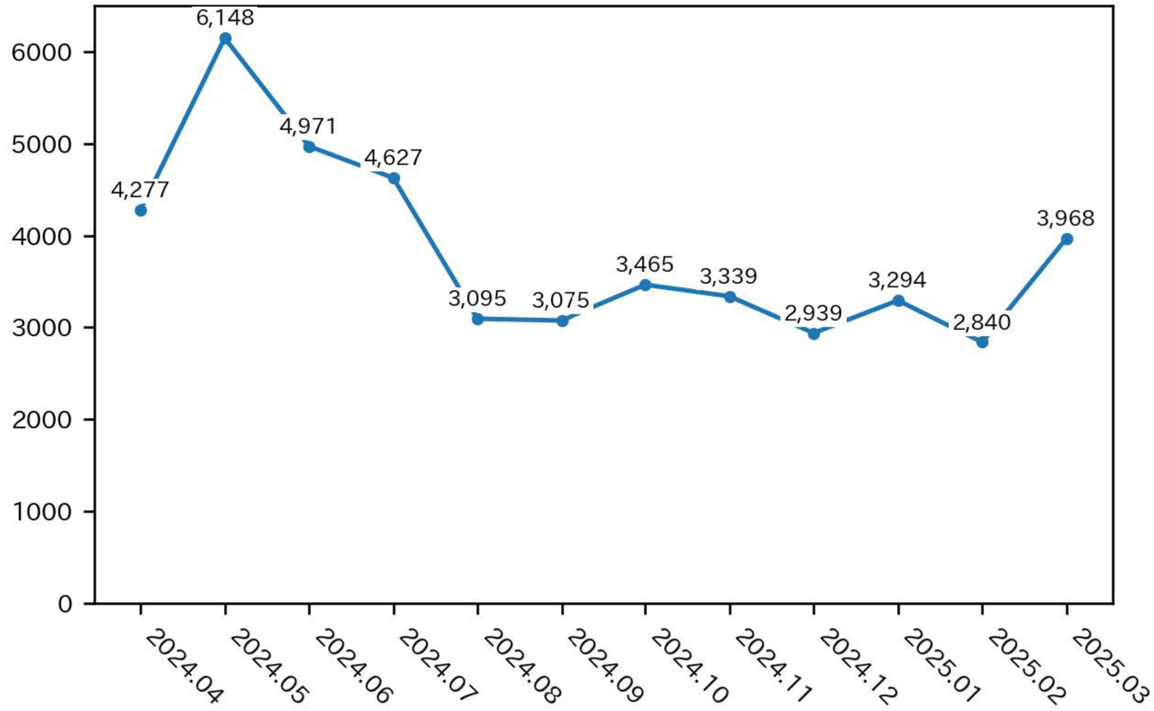
(2) "Number of Reports" refers to the total number of reports sent through the web form, e-mail or FAX.

(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.

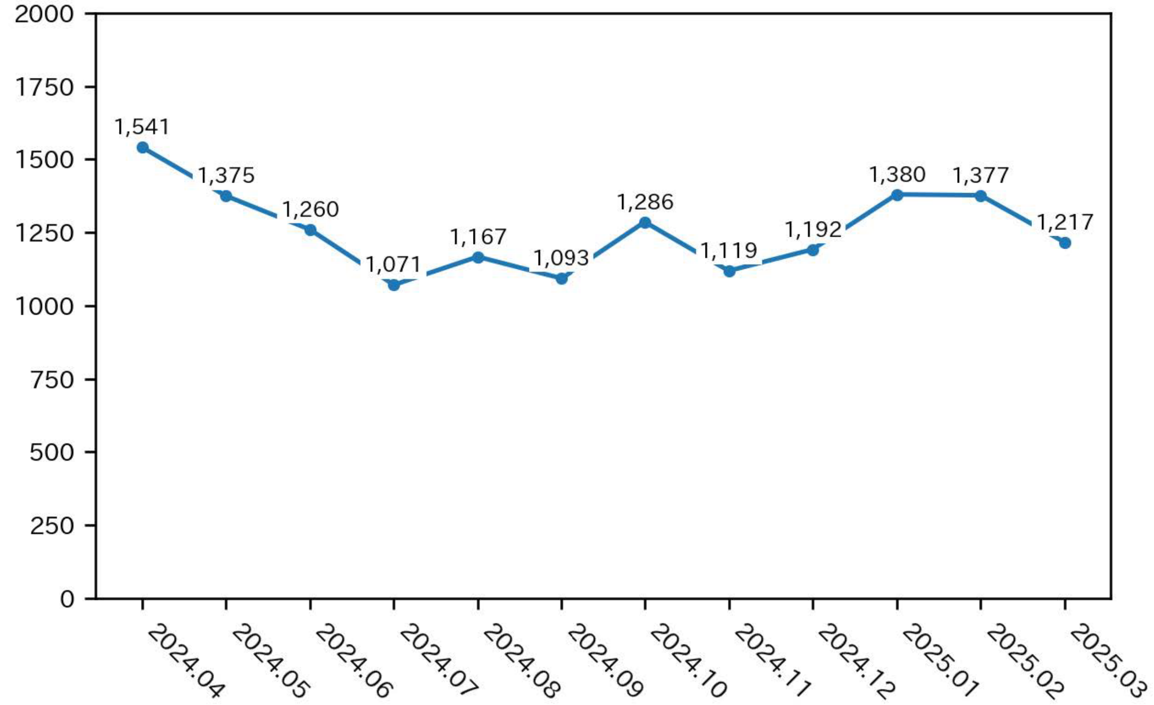
(4) "Number of Cases Coordinated" refers to the number of cases where coordination took place to prevent the spreading of an incident by sending them a report and asking the site administrator to address any issues.

[Chart 2.2 Number of incident reports by category]

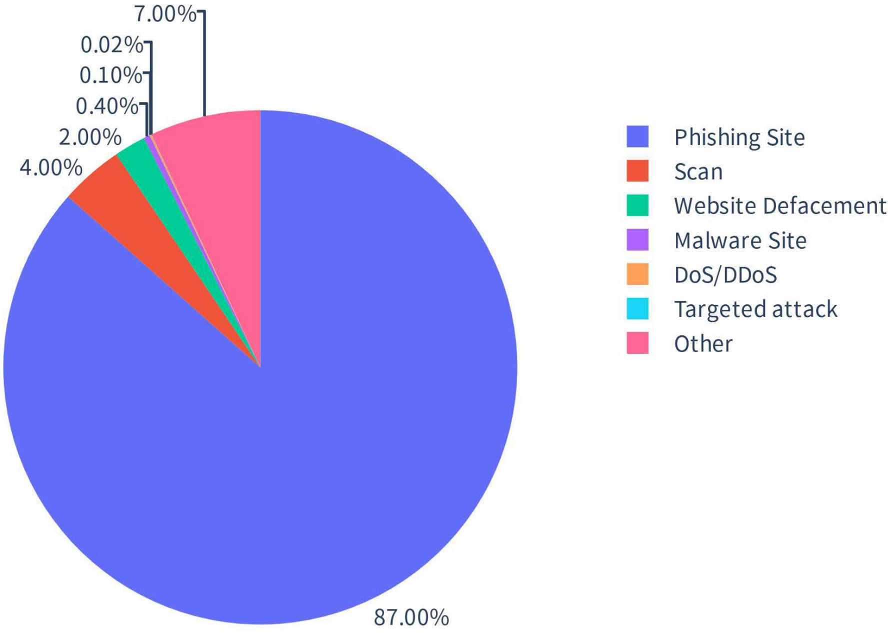
Incident Category	Jan	Feb	Mar	Total	Last Qtr.Total
Phishing Site	1,585	1,779	1,903	5,267	4,780
Website Defacement	53	25	17	95	53
Malware Site	10	1	12	23	36
Scan	105	72	79	256	233
DoS/DDoS	4	0	2	6	4
ICS Related	0	0	0	0	0
Targeted attack	1	0	0	1	2
Other	161	137	135	433	453



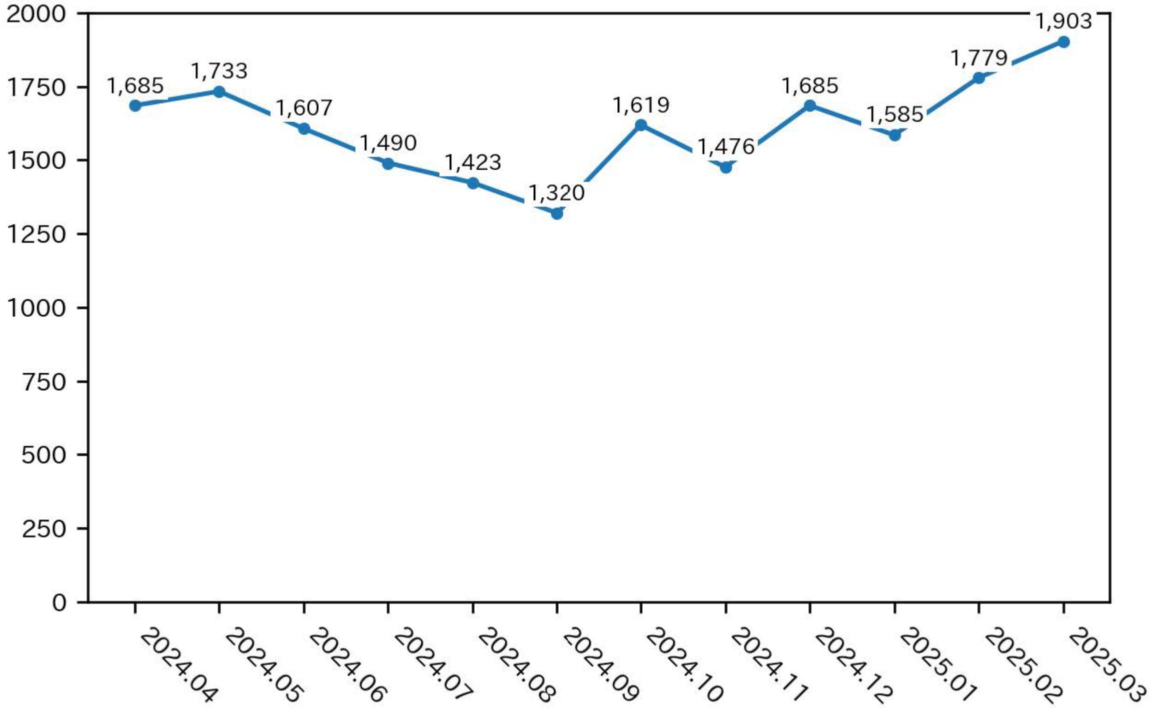
[Figure 2.1 Change in the number of incident reports]



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



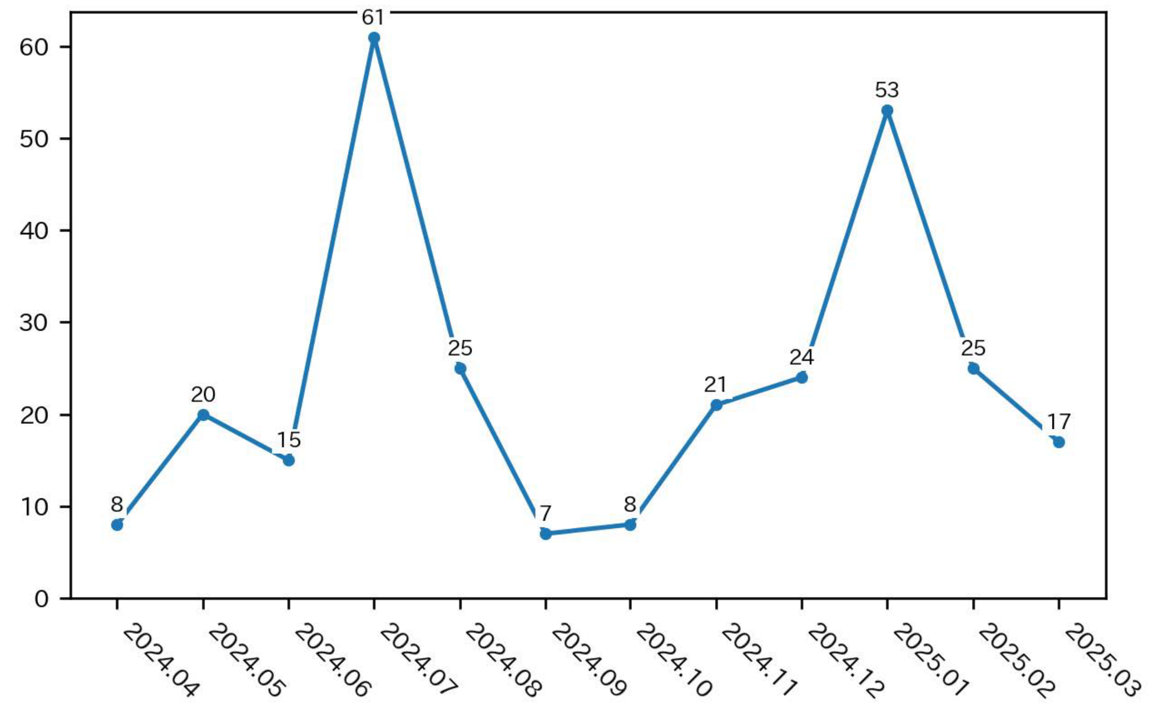
[Figure 2.3 Percentage of incidents by category]



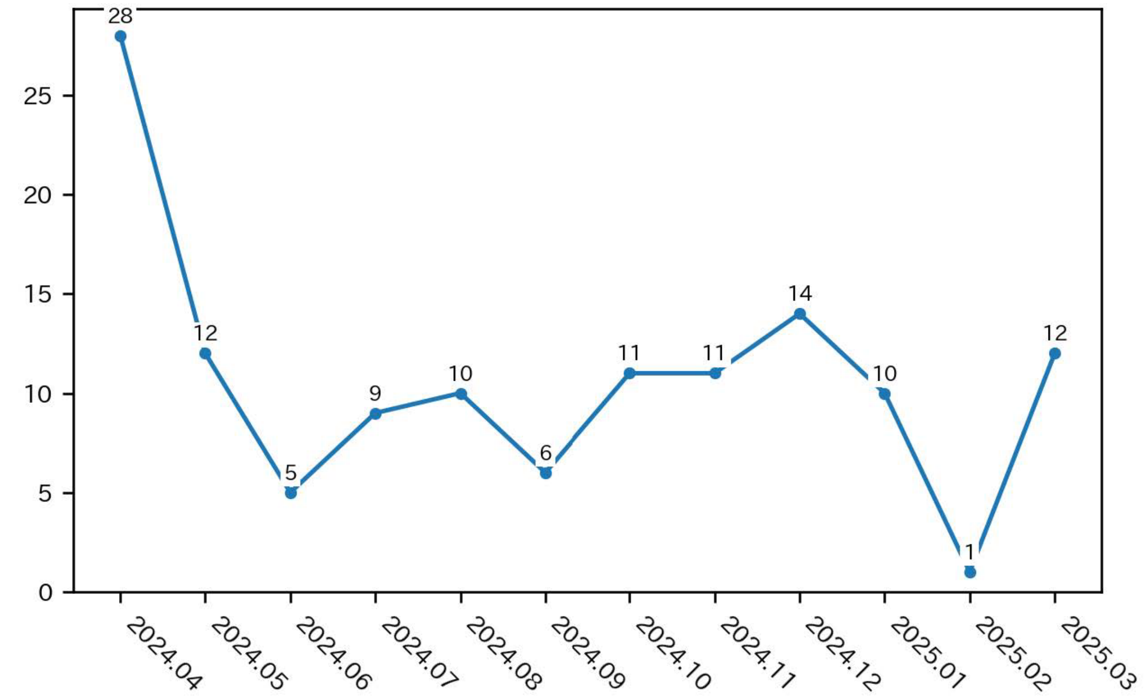
[Figure 2.4 Change in the number of phishing sites]

Incidents categorized as phishing sites accounted for 87%, and those categorized as scans, which search for vulnerabilities in systems, made up 4%.

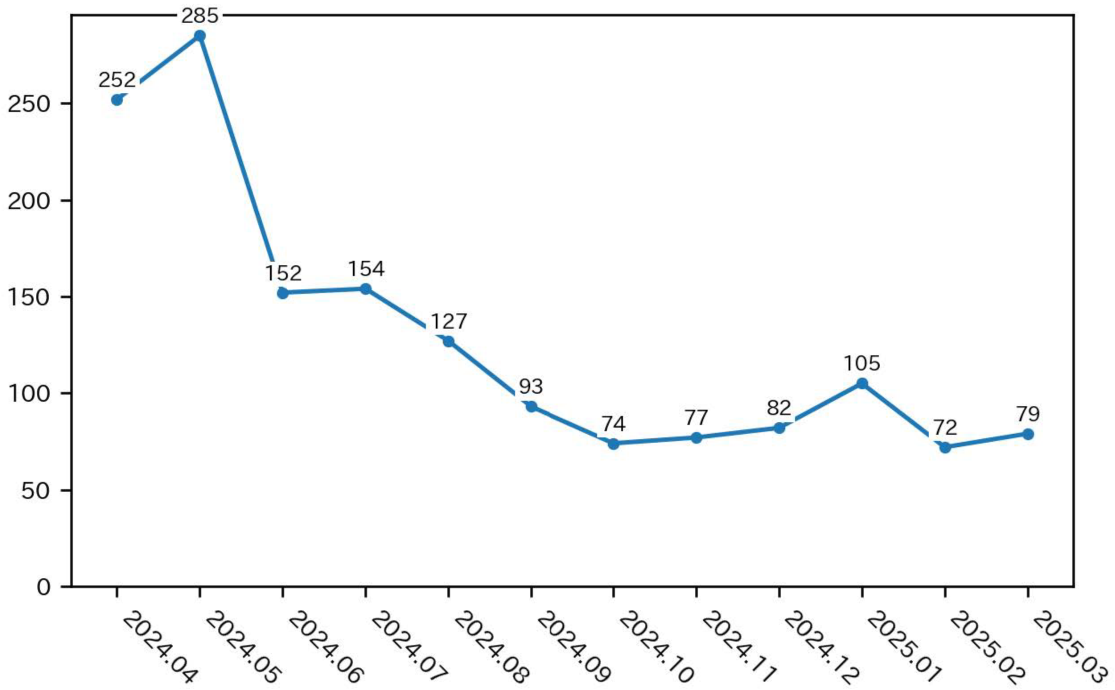
[Figure 2.4] through [Figure 2.7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



[Figure 2.5 Change in the number of website defacements]

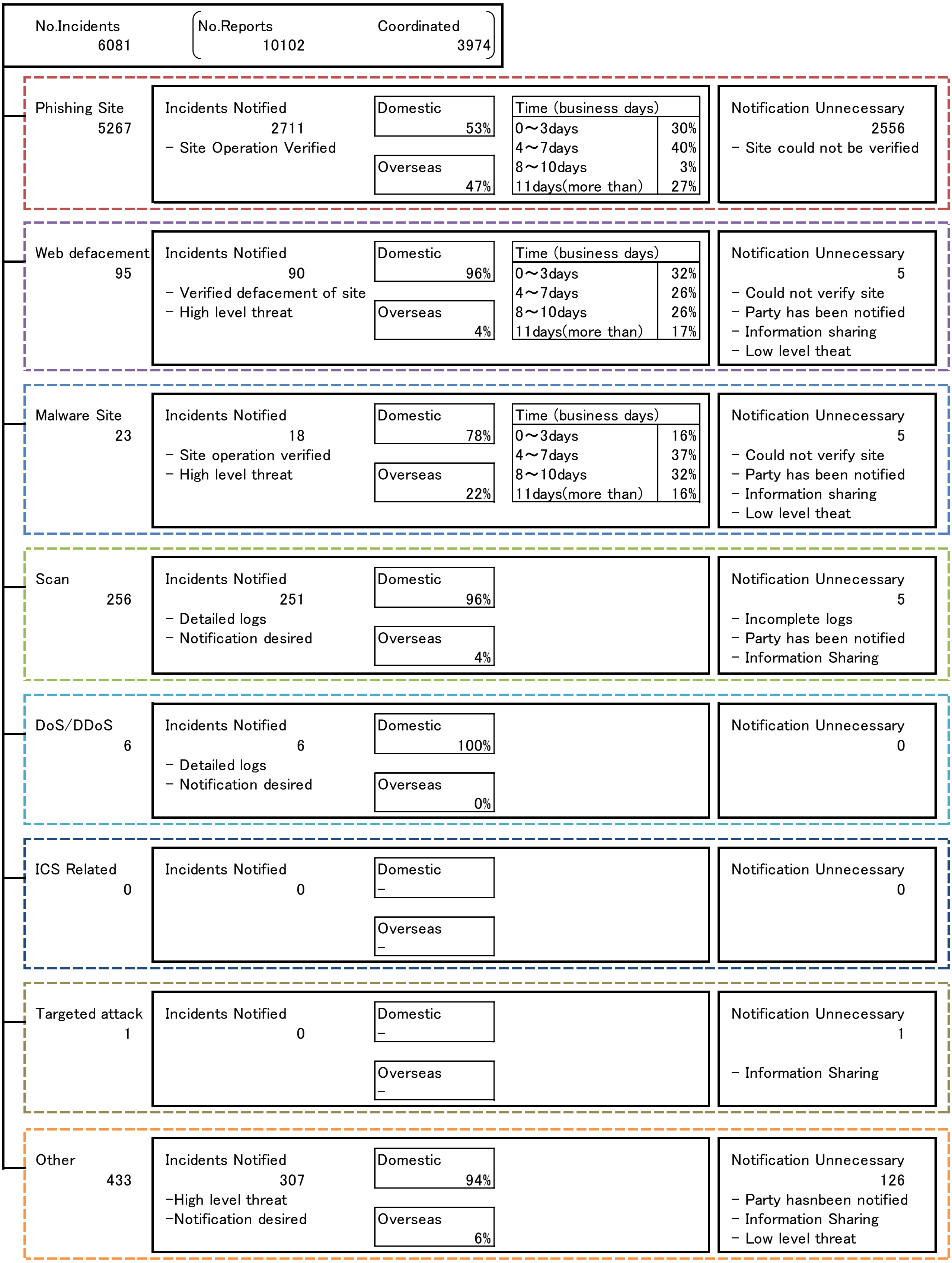


[Figure 2.6 Change in the number of malware sites]



[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.



No.Incidents 6081 | No.Reports 10102 | Coordinated 3974

Phishing Site
5267

Incidents Notified
2711
- Site Operation Verified

Domestic	53%
Overseas	47%

Time (business days)	
0～3days	30%
4～7days	40%
8～10days	3%
11days(more than)	27%

Notification Unnecessary
2556
- Site could not be verified

Web defacement
95

Incidents Notified
90
- Verified defacement of site
- High level threat

Domestic	96%
Overseas	4%

Time (business days)	
0～3days	32%
4～7days	26%
8～10days	26%
11days(more than)	17%

Notification Unnecessary
5
- Could not verify site
- Party has been notified
- Information sharing
- Low level theat

Malware Site
23

Incidents Notified
18
- Site operation verified
- High level threat

Domestic	78%
Overseas	22%

Time (business days)	
0～3days	16%
4～7days	37%
8～10days	32%
11days(more than)	16%

Notification Unnecessary
5
- Could not verify site
- Party has been notified
- Information sharing
- Low level theat

Scan
256

Incidents Notified
251
- Detailed logs
- Notification desired

Domestic	96%
Overseas	4%

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

DoS/DDoS
6

Incidents Notified
6
- Detailed logs
- Notification desired

Domestic	100%
Overseas	0%

Notification Unnecessary
0

ICS Related
0

Incidents Notified
0

Domestic	–
Overseas	–

Notification Unnecessary
0

Targeted attack
1

Incidents Notified
0

Domestic	–
Overseas	–

Notification Unnecessary
1
- Information Sharing

Other
433

Incidents Notified
307
-High level threat
-Notification desired

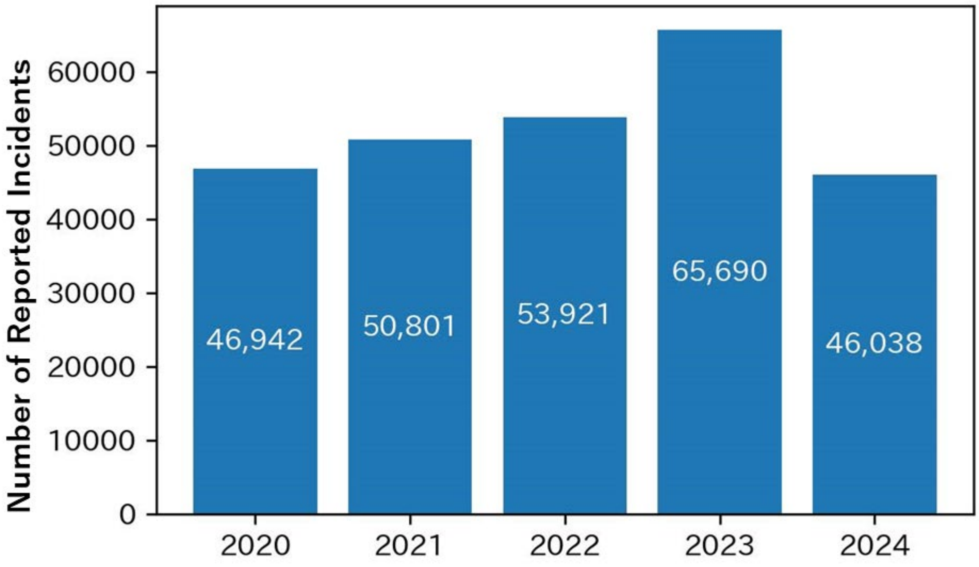
Domestic	94%
Overseas	6%

Notification Unnecessary
126
- Party hasnbeen notified
- Information Sharing
- Low level threat

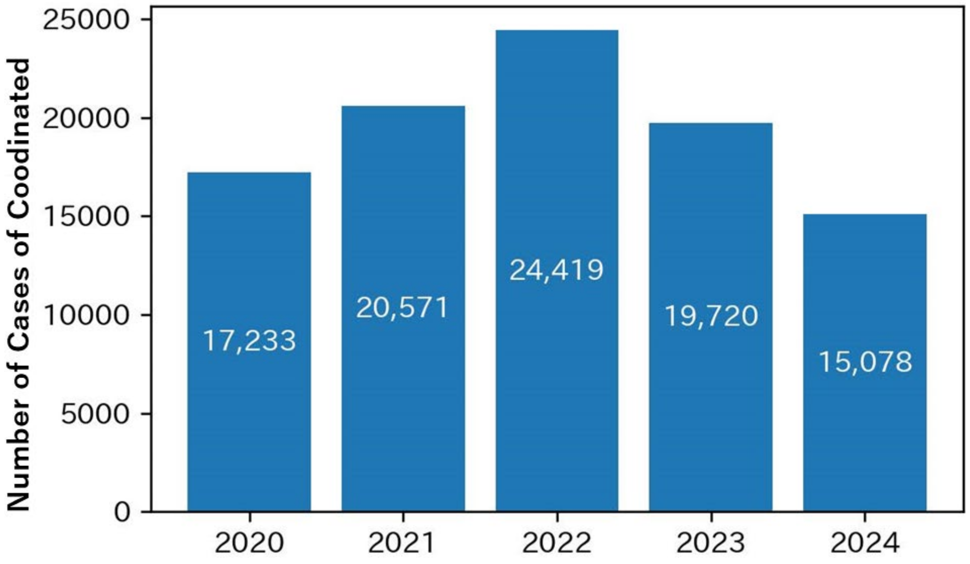
[Figure 2.8 Breakdown of incidents coordinated/handled]

3. Statistical Information by Fiscal Year

The annual numbers of reports and numbers of cases coordinated over the past five years up to this fiscal year are shown in[Figure 3.1] and [Figure 3.2], respectively. (Each fiscal year begins on April 1 and ends on March 31 of the following year.) The total number of reports received in FY2024 was 46,038, decreasing 30% year on year from 65,690. The total number of cases coordinated in FY2024 was 15,078, decreasing 24% year on year from 19,720.



[Figure 3.1 : Change in the total number of reports (by fiscal year)]



[Figure 3.2 : Change in the total number of cases coordinated (by fiscal year)]

4. Incident Trends

4.1. Phishing Site Trends

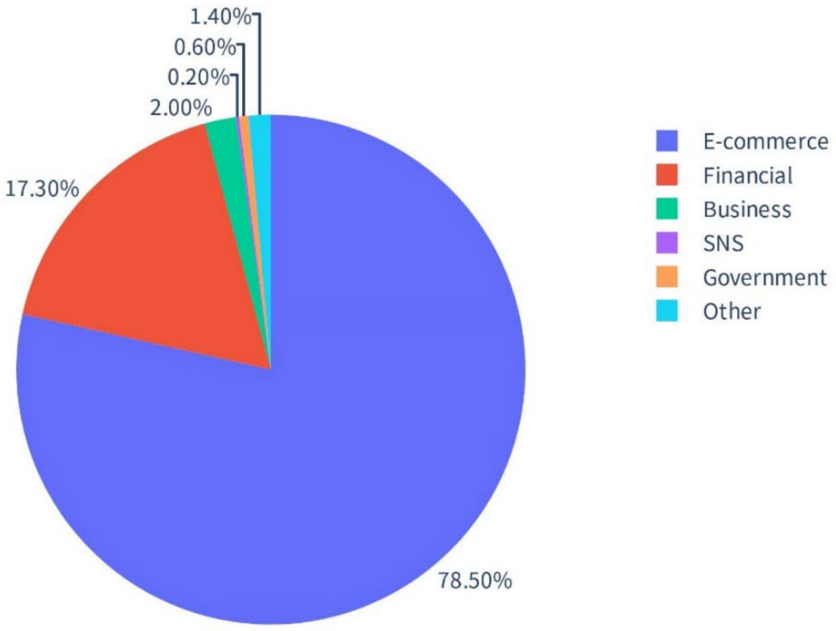
During this quarter, 5,267 reports on phishing sites were received, representing a 10% increase from 4,780 in the previous quarter. This marks a 10% increase from the same quarter last year (4,781).

During this quarter, there were 502 phishing sites that spoofed overseas brands, which is roughly the same as 504 in the previous quarter. There were 4,277 phishing sites that spoofed domestic brands, increasing 16% from 3,690 in the previous quarter. The numbers of phishing sites reported in this quarter for overseas and domestic brands are shown in [Chart 4.1]. The percentages of phishing sites reported in this quarter by industry for overseas and domestic brands are shown in [Figure 4.1] [Figure 4.2].

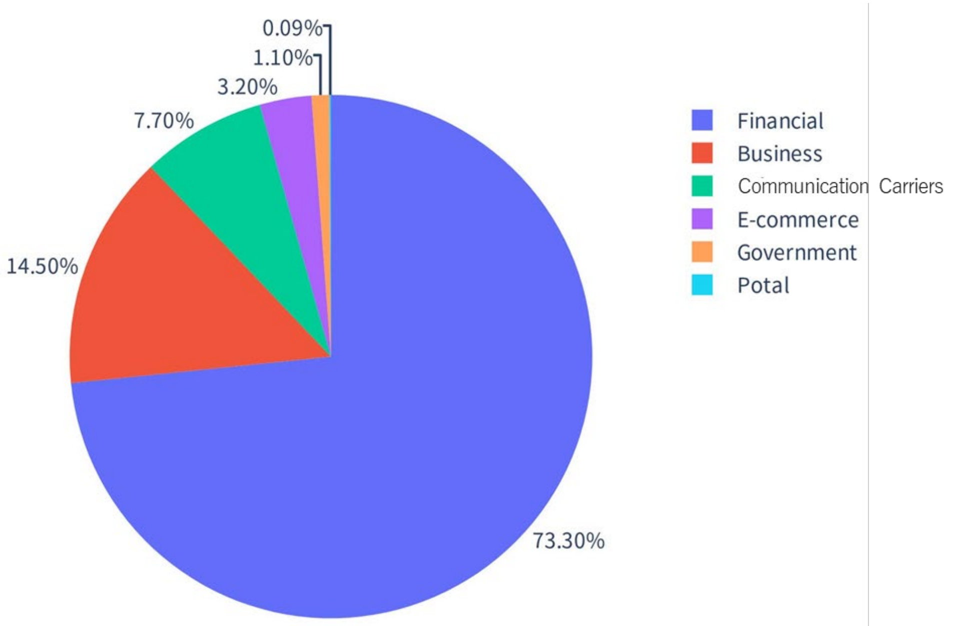
[Chart 4.1 Number of phishing sites for domestic and overseas brands]

Phishing Site	Jan	Feb	Mar	Domestic/Overseas Total (%)
Domestic Brand	1,270	1,424	1,583	4,277 (81%)
Overseas Brand	160	175	167	502 (10%)
Unknown Brand (5)	155	180	153	488 (9%)
Monthly Total	1,585	1,779	1,903	5,267

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



[Figure 4.1 Percentage of reported phishing sites by industry for overseas brands]



[Figure 4.2 Percentage of reported phishing sites by industry for domestic brands]

Out of the total number of phishing sites reported to JPCERT/CC, 78.5% spoofed e-commerce websites for overseas brands and 73.3% spoofed financial websites for domestic brands, both representing the largest share respectively. For overseas brands, phishing sites spoofing Amazon accounted for around 60% of the phishing sites reported. For domestic brands, phishing sites spoofing Credit Saison, Sumitomo Mitsui Card and JCB were reported in large numbers. The websites that JPCERT/CC coordinated with to take down phishing sites were 53% domestic and 47% overseas for this quarter, indicating an increase in domestic parties compared to the previous quarter (domestic: 36%, overseas: 64%).

4.2. Website Defacement Trends

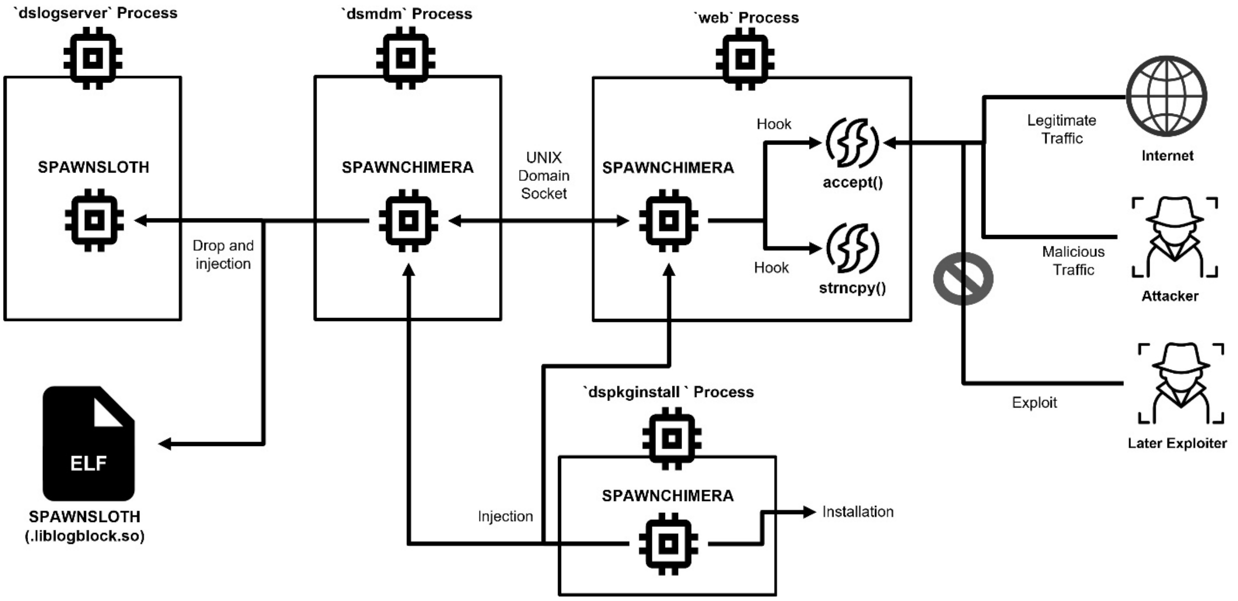
The number of website defacements reported in this quarter was 95. This was a 75% increase from 53 in the previous quarter.
During this quarter, JPCERT/CC confirmed the following cases of website defacements.

1.Redirecting users who accessed a website to a suspicious shopping site
- Alteration and fraudulent placement of a .htaccess file
- Insertion of code redirecting to a PHP file

2.Insertion of code for mining cryptocurrency into a website

3.Insertion of adware written in JavaScript into a website

In case 1, .htaccess files placed in web server directories were altered or fraudulently placed in numerous directories. Malicious .htaccess files contained, for example, settings restricting access to files with a certain extension, or redirecting users to a PHP file placed by the attacker.



[Figure 4.3 Flow of SPAWNCHIMERA's behavior]

PHP files placed by the attacker contained code that redirects users to a fake shopping site, or code that executes code obtained from a C2 server on a web server. PHP backdoors capable of sending files to a C2 server were also installed.

4.3. Targeted Attack Trends

There were 1 incidents categorized as a targeted attack. We will discuss it below.

4.3.1. Attack exploiting a vulnerability in Ivanti Connect Secure (CVE-2025-0282)

During this quarter, a number of Japanese organizations reported being subjected to an attack exploiting a vulnerability in Ivanti Connect Secure (CVE-2025-0282). These cases were detected due to the occurrence of suspicious ICMP communication from the organization's Ivanti Connect Secure to its internal network, and an integrity checker tool identified the placement of multiple malicious files. JPCERT/CC confirmed that these files were SPAWNCHIMERA malware, which combines the functions of SPAWNSNAIL, SPAWNMOLE, and SPAWNANT malware used by an attack group known as UNC5221, which was reported by Google in April 2024.
The flow of the installed SPAWNCHIMERA's behavior is shown in [Figure 4.3].

4.4. Other Incident Trends

The number of malware sites reported in this quarter was 23. This was a 36% decrease from 36 in the previous quarter.
The number of scans reported in this quarter was 256. This was a 10% increase from 233 in the previous quarter. The top 10 ports that the scans targeted are listed in [Chart4.2]. Ports targeted frequently were Telnet (23/TCP), SSH (22/TCP), HTTP (80/TCP) and 88/TCP.
There were 433 incidents categorized as others. This was a 4% decrease from 453 in the previous quarter.

[Chart 4.2 Top 10 ports by number of scans]

Port	Jan	Feb	Mar	Total
23/tcp	29	55	49	133
22/tcp	9	4	10	23
80/tcp	7	1	1	9
88/tcp	6	1	1	8
8080/tcp	5	0	3	8
79/tcp	4	2	2	8
9001/tcp	3	0	3	6
9000/tcp	4	0	1	5
81/tcp	4	0	1	5
8081/tcp	4	0	1	5

5. Incident Handling Case Examples

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

5.1. Notification to Japanese organizations potentially compromised due to a vulnerability in Ivanti Connect Secure (CVE-2025-0282)

As discussed in chapter 4, JPCERT/CC received reports of damage due to this vulnerability from a number of organizations. Some of the organizations even had alterations intended to prevent the integrity checker tool provided by Ivanti to check for evidence of compromise from conducting investigations properly. In response, JPCERT/CC issued a security alert and published the analysis results of malware found in some of the organizations.

Security alert concerning a vulnerability in Ivanti Connect Secure, etc. (CVE-2025-0282)
https://www.jpcert.or.jp/at/2025/at250001.html (Japanese only)

SPAWNCHIMERA Malware: The Chimera Spawning from Ivanti Connect Secure Vulnerability
https://blogs.jpcert.or.jp/en/2025/02/spawnchimera.html

Using information received from an external organization on the addresses of devices potentially compromised due to exploitation of this vulnerability, JPCERT/CC requested system administrators in Japan using these devices to check their devices.

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.)

If you would like to cite or reprint this document, please contact the Public Relations of JPCERT/CC (pr@jpcert.or.jp). Company names and product names in this document are the trademarks or registered trademarks of the respective companies.

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 [January 1, 2025 - March 31, 2025]

- First version issued: April 17, 2025
- 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