JPCERT CC®

JPCERT/CC Quarterly Report

April 1, 2025 ～ June 30, 2025

July 17, 2025

JPCERT Coordination Center

Until fiscal year 2024, JPCERT/CC published a quarterly report titled "JPCERT/CC Quarterly Activity Report" in Japanese. This report provided an overview of the various activities undertaken by JPCERT/CC. An English publication, "JPCERT/CC Activities Overview Topics," was also offered as a partial translation of the Japanese original. Starting in fiscal year 2025, the JPCERT/CC Quarterly Activity Report and the Incident Handling Report were integrated into a new report titled "JPCERT/CC Quarterly Report." The newly integrated report will be offered in both Japanese and English.

Disclaimer

This English version was produced using machine translation and has undergone only minimal human review. Please note that the translations of proper nouns — including the names of organizations, projects, frameworks, documents, contracts, and committees — are provided for convenience and may not be fully accurate. In the event of any discrepancies or ambiguities, the Japanese original shall be regarded as the authoritative version. The original Japanese version is available at: https://www.jpcert.or.jp/qr/

Contents

Introduction

JPCERT Coordination Center (herein, JPCERT/CC) 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.).

Most of 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 2025 Fiscal Year," or the Cabinet Secretariat as part of the "Verification Activities Concerning Methods to Facilitate the Collection of Technical Information on Attacks from Affected Organizations."

This document reports on activities undertaken between April 1 and June 30, 2025.

Note that "Chapter 5 Domestic Collaboration Activities," "Chapter 6 International Collaboration Activities," "Chapter 7 Council of Anti-Phishing Japan Activities," and "Chapter 8 Public Relations Activities" contain information on voluntary activities other than sponsored activities.

Topics & Highlights

Newly Redesigned JPCERT/CC Quarterly Report

JPCERT/CC's activities begin with coordinating between relevant parties in an incident, and critical information based on the knowledge gained through individual coordination used to be published to alert the public at large. Later, with the aim of further publicizing JPCERT/CC and its activities, it began publishing periodic reports that provided an overview of its activities. As JPCERT/CC expanded its operations to cover coordination of vulnerability information, Internet threat monitoring, and other activities, its activity overviews were upgraded into a more comprehensive report titled JPCERT/CC Quarterly Activity Report, which reported the full range of its operations.

JPCERT/CC's operations must always address the question of who should be provided with what information and at what timing. The constant effort to find the most suitable answer to this question for each operation and act accordingly has shaped JPCERT/CC's activities. The current JPCERT/CC Quarterly Activity Report provide an overview of these activities.

Unlike the time when JPCERT/CC was launched, a wide variety of security information is available

in the world today. For this reason, people who deal with cyber security need to select and use the appropriate information in a timely manner, according to their roles and situation. JPCERT/CC has reviewed and improved its activities from time to time so that it can contribute to the efforts of such people. In recent years, incident handling has become increasingly associated and integrated with other operations. In light of these circumstances, JPCERT/CC decided to integrate the JPCERT/CC Quarterly Activity Report and the Incident Handling Report from FY2025 to better publicize itself and its activities, with the aim of facilitating the use of information and services it provides.

JPCERT/CC strives to maximize the results of commissioned operations, primarily those 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 2025 Fiscal Year," and the Cabinet Secretariat as part of the "Verification Activities Concerning Methods to Facilitate the Collection of Technical Information on Attacks from Affected Organizations," in addition to voluntary activities. To that end, these activities are carried out in an integrated manner while appropriately separating and managing invested resources. JPCERT/CC will continue to make improvements to ensure the valuable knowledge gained through individual operations and the overview of its activities are communicated to the readers in a well-balanced manner.

JPCERT/CC staff member is re-elected to the Board of FIRST

Yukako Uchida, manager of the Global Coordination Division, ran for the board of the Forum of Incident Response and Security Teams (FIRST) and was elected for the third time. FIRST is the world's largest community boasting a membership of 808 CSIRTs from 113 countries and economies as of June 2025. JPCERT/CC was the first in Japan to become a member of FIRST in 1998 and has actively participated in its activities to collaborate with overseas CSIRTs since then.

Planning for its activities is handled by the 10 members on its Board of Directors. The Board serve a 2-year term, and half of them are elected each year through voting by participating organizations. At the annual conference held in Copenhagen, Denmark in June, the results of the online voting were announced, and 5 new directors including Uchida were elected. We believe the voting results were helped by the trust built through the recognition of JPCERT/CC's ongoing contribution to FIRST. Also, it is worth noting that Uchida continues to be the only member from Asia to serve on the board, which mostly consists of members from Europe and the United States.

Upon her reelection, Uchida commented, "Ever since the FIRST conference was held in Fukuoka in 2024, I feel that interest in FIRST has been rising in Japan as well. I intend to redouble my efforts to keep this momentum alive as we further promote FIRST activities in Japan and other parts of Asia, including holding events, and encourage more organizations to use it as a venue for international cooperation."

Please refer to the link below for information about other Board members and past directors.

- FIRST.Org,Inc., Board of Directors

https://www.first.org/about/organization/directors

Chapter 1

Incident Response Support

JPCERT/CC receives reports on computer security incidents (herein, incidents) that occur inside and outside Japan[*1]. This chapter will introduce incident reports received during the period from April 1, 2025 through June 30, 2025, from both quantitative and qualitative perspectives using statistics and case examples.

1.1 Quarterly Statistics

Table 1.1[*2] 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 14,558. Of these, the number of cases that JPCERT/CC coordinated was 3,544. When compared with the previous quarter, the number of reports increased by 44%, and the number of cases coordinated decreased by 11%. Year on year (15,396 reports received, 4,176 cases coordinated), the number of reports decreased by 5% and the number of cases coordinated decreased by 15%.

Figure 1.1, 1.2 show the monthly changes in the total number of reports and incident cases coordi-

Table 1.1 Number of incident reports

	Apr	May	Jun	Total	Last Qtr.Total
Number of Reports	4,053	4,277	6,228	14,558	10,102
Number of Incident	2,532	2,574	3,242	8,348	6,081
Cases Coordinated	1,186	1,013	1,345	3,544	3,974

[*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**.

[*2] **Number of reports** refers to the total number of reports sent through the web form, e-mail or FAX. **Number of incidents** refers to the number of incidents contained in each report. Multiple reports on the same incidents are counted as 1 incident. **Number of 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.

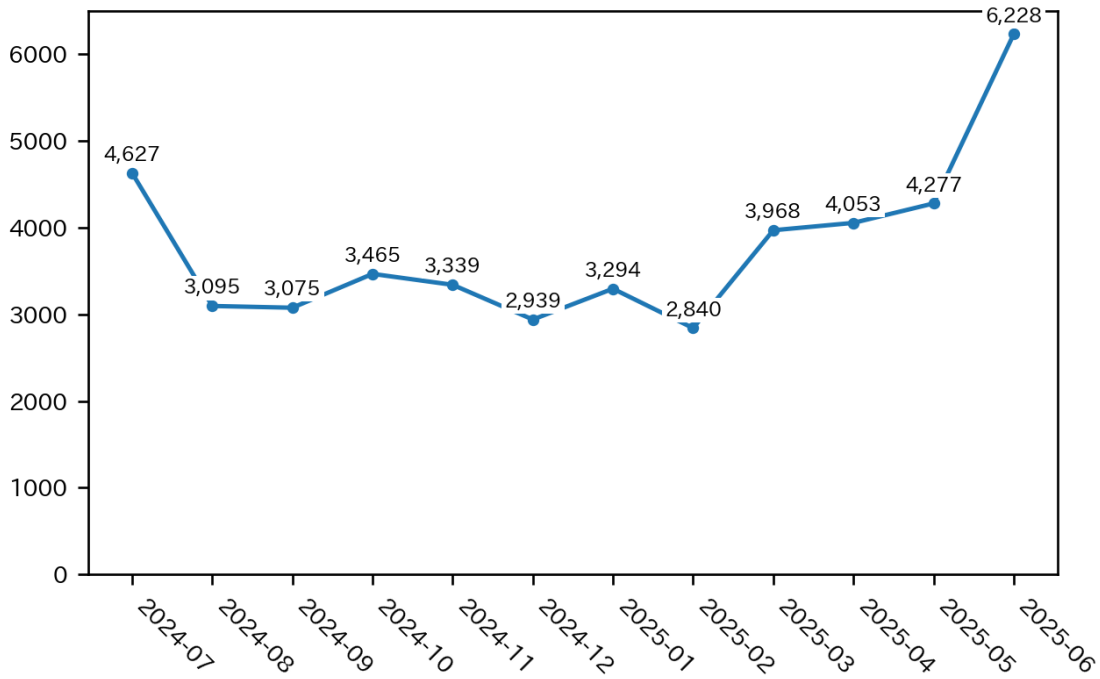

Figure 1.1 Change in the number of incident reports

Table 1.2 Number of incident reports by category

Incident Category	Apr	May	Jun	Total	Last Qtr.
Phishing Site	2,222	2,256	2,880	7,358	5,267
Website Defacement	26	64	141	231	95
Malware Site	6	18	4	28	23
Scan	90	88	62	240	256
DoS/DDoS	0	2	0	2	6
ICS Related	0	0	0	0	0
Targeted attack	1	2	2	5	1
Other	187	144	153	484	433

nated 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 A Incident Categories**. Table 1.2 shows a breakdown of the number of incidents reported during the quarter by category. A breakdown of the percentage is shown in Figure 1.3.

Incidents categorized as phishing sites accounted for 88%, and those categorized as scans, which search for vulnerabilities in systems, made up 3%.

Figure 1.4–1.7 show the monthly changes in the number of incidents categorized as phishing sites,

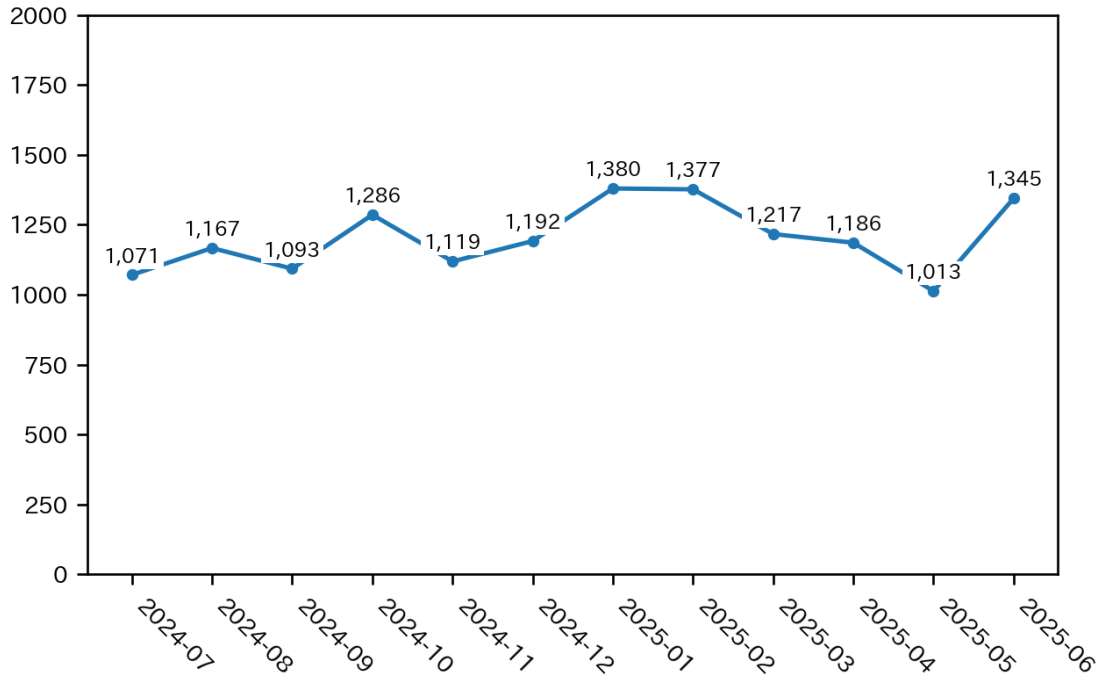

Figure 1.2 Change in the number of incident cases coordinated

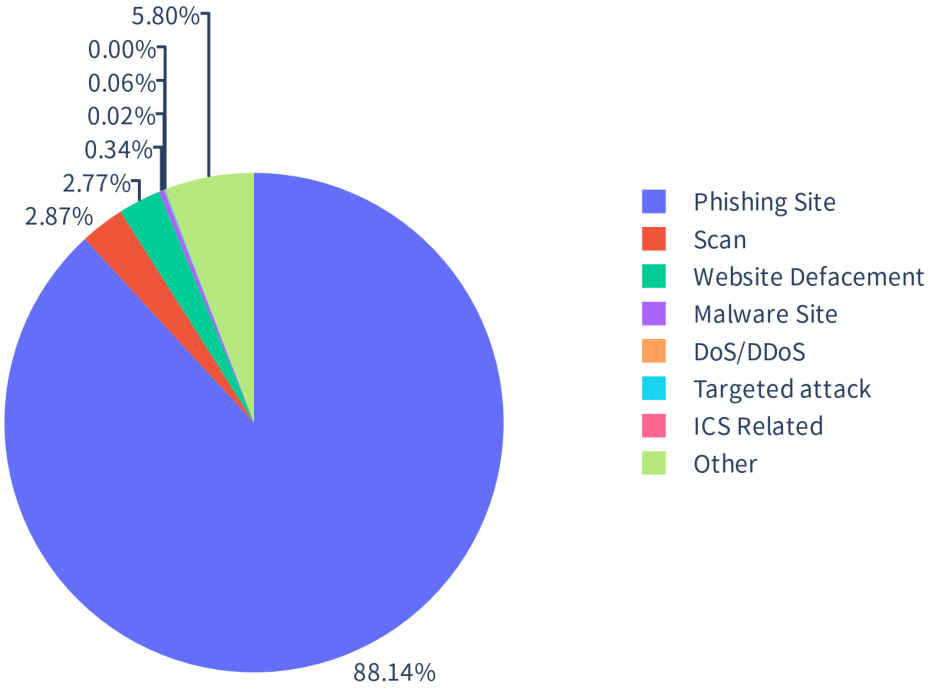

Figure 1.3 Percentage of incidents by category

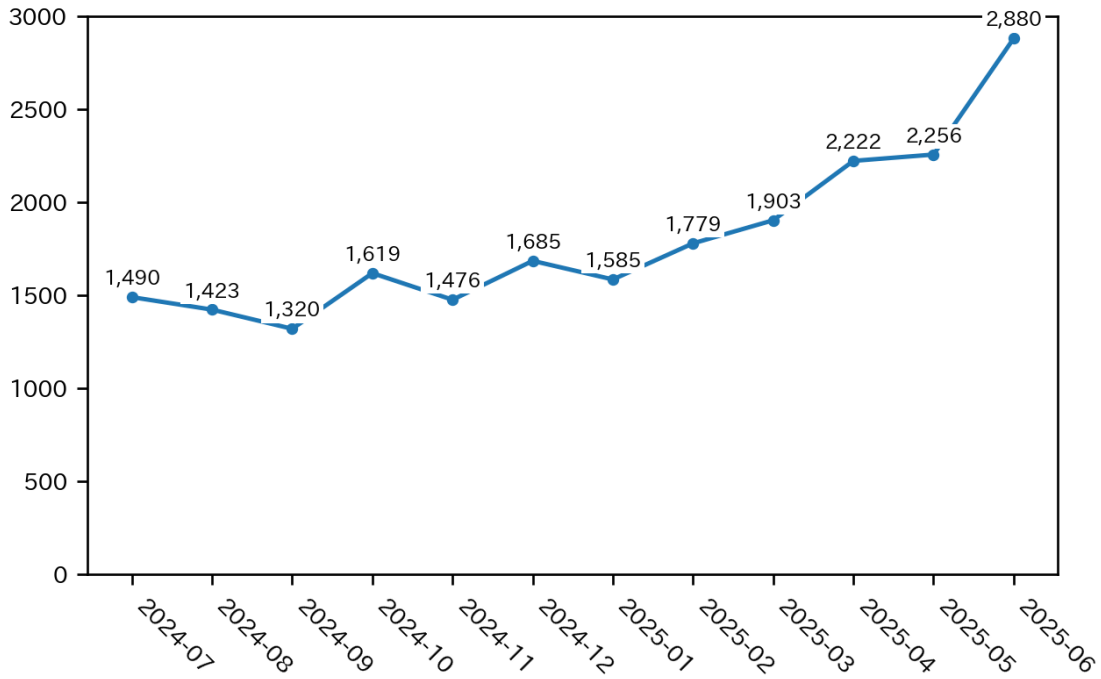

Figure 1.4 Change in the number of phishing sites

website defacement, malware sites and scans over the past year.

Figure 1.8 provides an overview as well as a breakdown of the incidents that were coordinated /Handled.

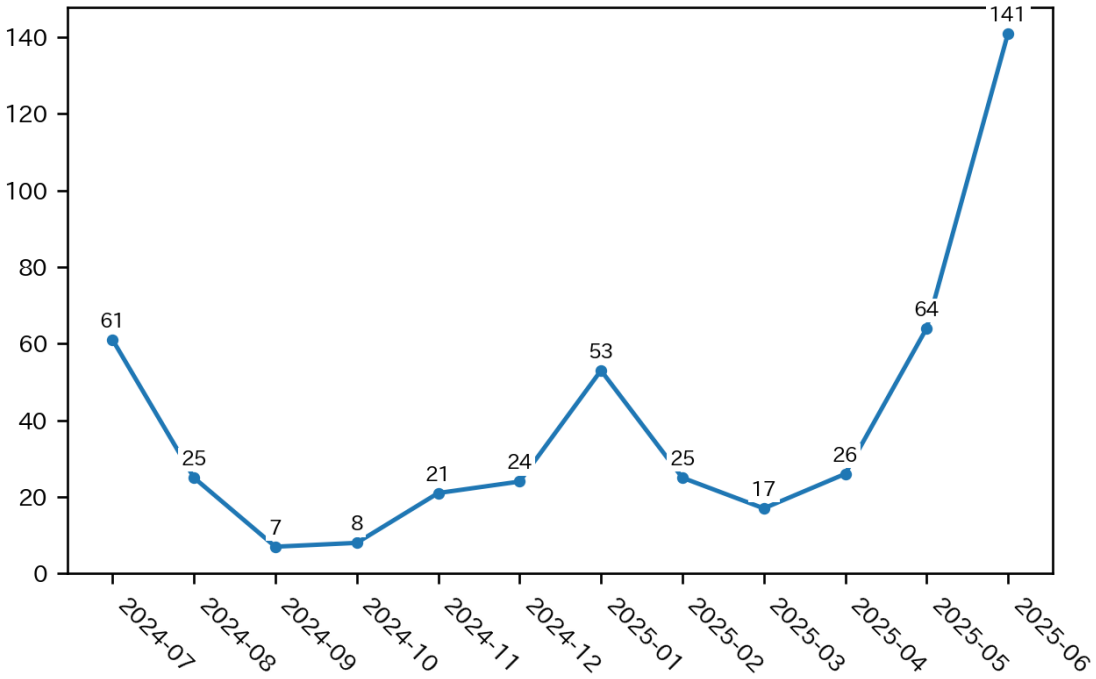

Figure 1.5 Change in the number of website defacements

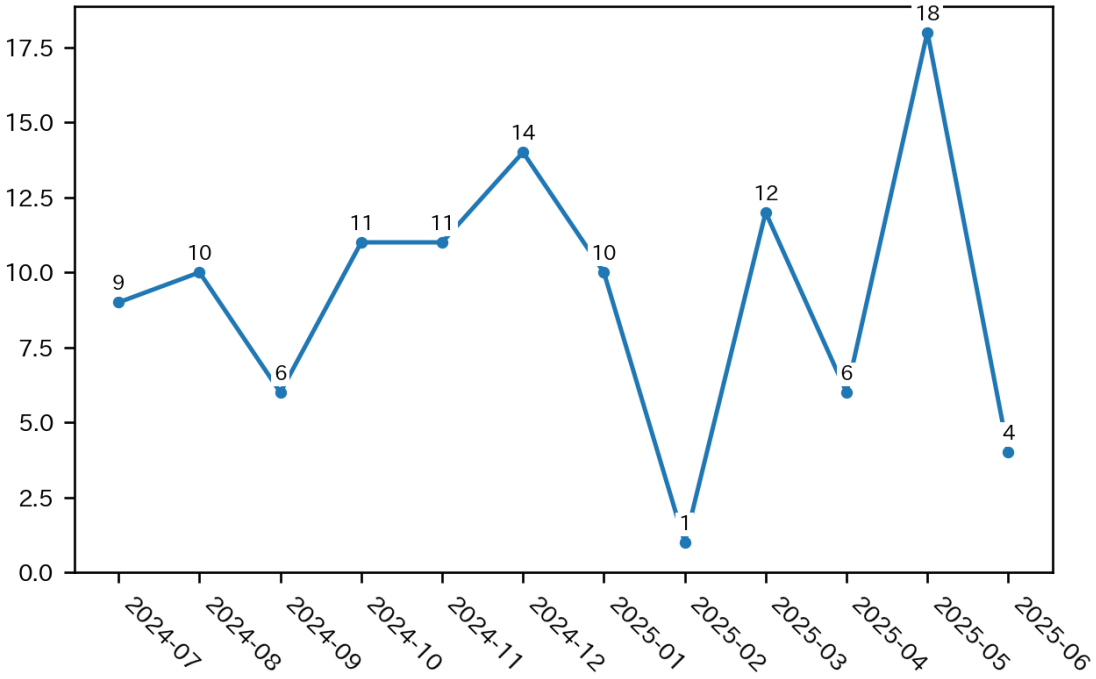

Figure 1.6 Change in the number of malware sites

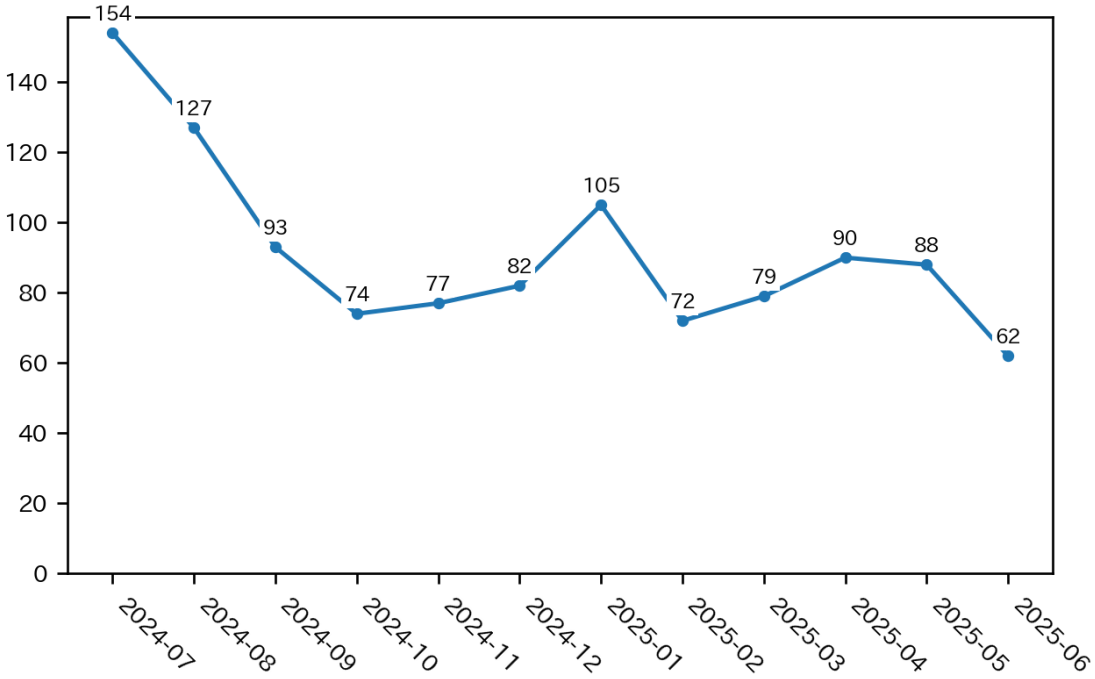

Figure 1.7 Change in the number of scans

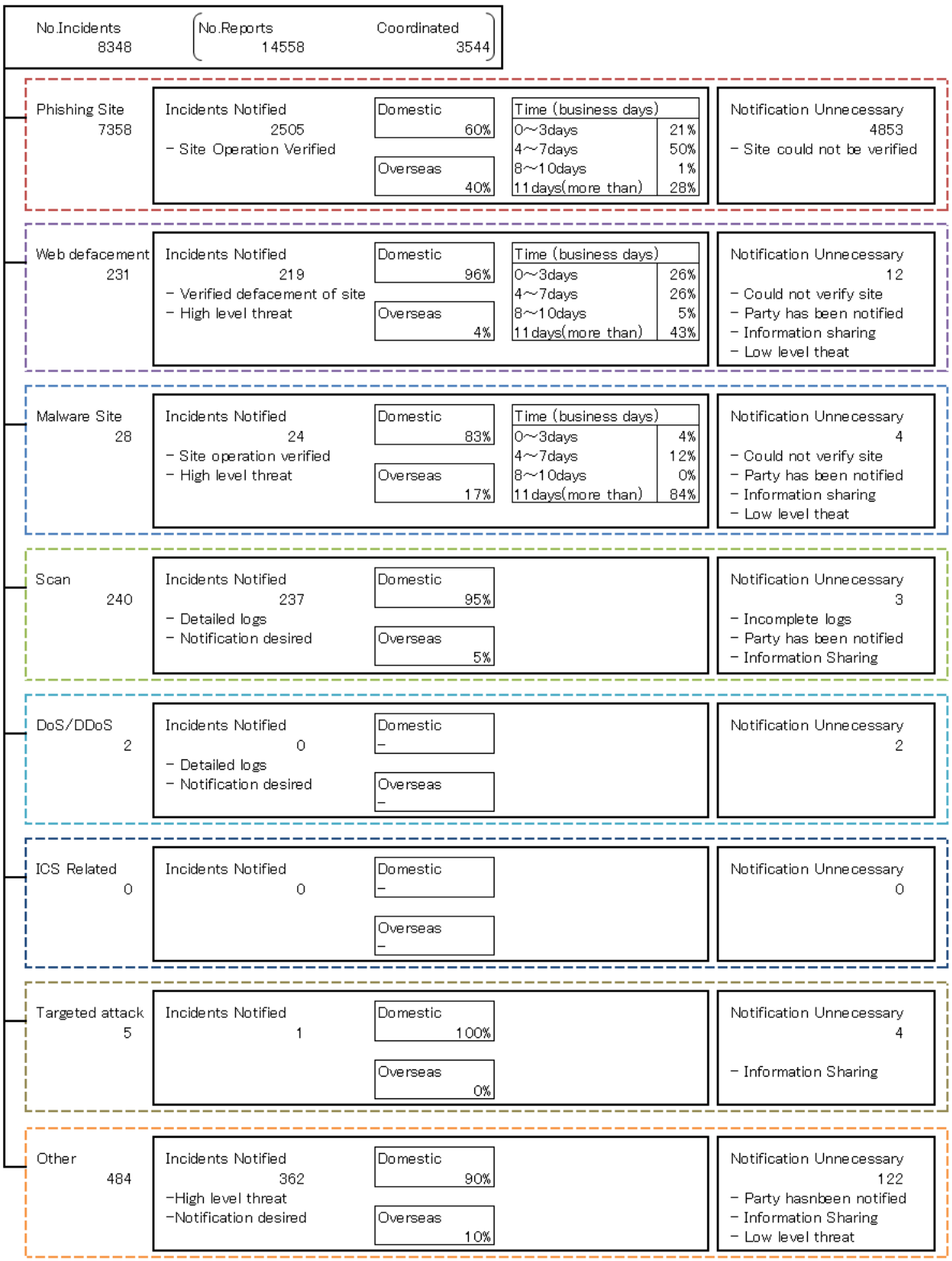

Figure 1.8 Breakdown of incidents coordinated/handled

Table 1.3 Number of phishing sites for domestic and overseas brands

Phishing Site	Apr	May	Jun	Total	Pct.
Domestic Brand	1,880	1,731	2,339	5,950	81%
Overseas Brand	109	194	282	585	8%
Unknown Brand	233	331	259	823	11%
Monthly Total	2,222	2,256	2,880	7,358	

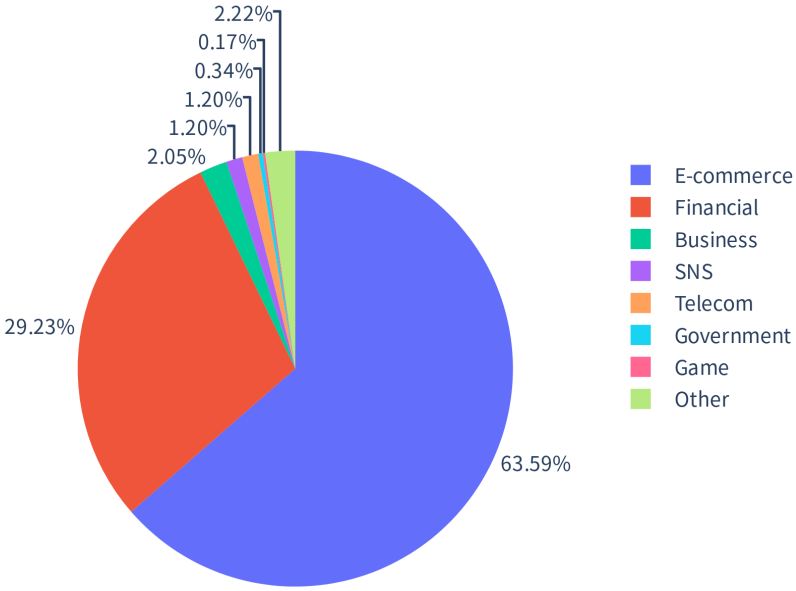

Figure 1.9 Percentage of reported phishing sites by industry for overseas brands

1.2 Incident Trends

1.2.1 Phishing Site Trends

During this quarter, 7,358, reports on phishing sites were received, representing a 40% increase from 5,267 in the previous quarter. This marks a 46% increase from the same quarter last year (5,025).

During this quarter, there were 585 phishing sites that spoofed overseas brands, increasing 17% from 502 in the previous quarter. There were 5,950 phishing sites that spoofed domestic brands, increasing 39% from 4,277 in the previous quarter. The numbers of phishing sites reported in this quarter for overseas and domestic brands are shown in Table 1.3[*3]. The percentages of phishing sites reported in this quarter by industry for overseas and domestic brands are shown in Figure 1.9, 1.10.

Out of the total number of phishing sites reported to JPCERT/CC, 63.6% spoofed e-commerce websites for overseas brands and 70.2% spoofed financial websites for domestic brands, both representing

[*3] **Unknown brand** refers to sites which could not be verified since the reported site had already been suspended when accessed for confirmation.

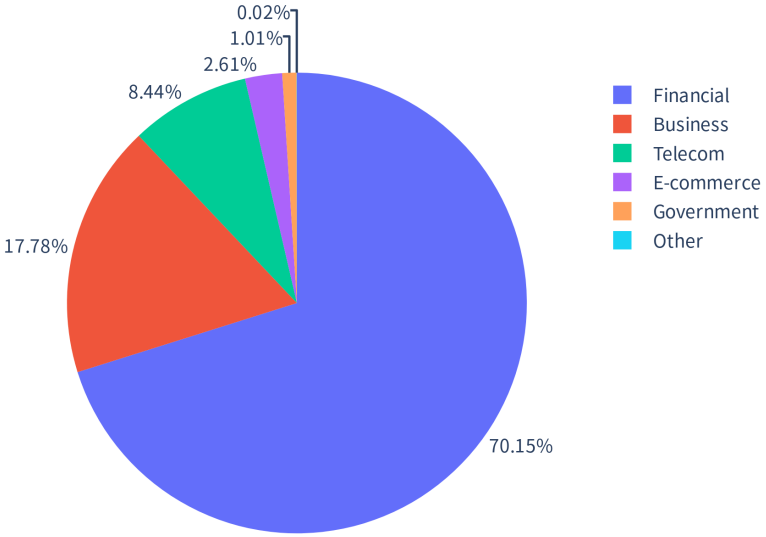

Figure 1.10 Percentage of reported phishing sites by industry for domestic brands

the largest share respectively.

For overseas brands, phishing sites spoofing Amazon and Apple ID accounted for around 60% of the phishing sites reported. For domestic brands, phishing sites spoofing SBI Securities, JCB, Sumitomo Mitsui Card, and Rakuten were reported in large numbers. The websites that JPCERT/CC coordinated with to take down phishing sites were 60% domestic and 40% overseas for this quarter, indicating an increase in domestic parties compared to the previous quarter (domestic 53%, overseas 47%).

1.2.2 Website Defacement Trends

The number of website defacements reported in this quarter was 231. This was a 143% increase from 95 in the previous quarter.

During this quarter, JPCERT/CC confirmed the following cases of website defacements.

1. Insertion of code for displaying a fake CAPTCHA on a website
2. Planting of a malicious WordPress plugin on a website

In case 1, when a user accesses the compromised website, a fake CAPTCHA checkbox (Figure 1.11) pretending to verify that the user is not a robot is displayed. If the checkbox is checked, a message is shown urging the user to press the Windows key + R, which opens a verification window. The user is then urged to press Ctrl + V in the window and press Enter to finish the verification. If the user follows these steps, a command copied to the clipboard by the script gets executed. The executed command is an mshta command with a suspicious URL designated as an argument, and it is apparently intended to download and run malicious code. This type of method in which the attacker attempts to trick the user into executing malicious code is called ClickFix.

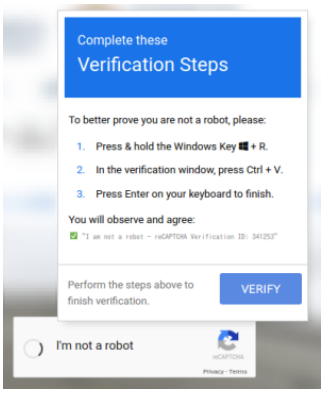

Figure 1.11 ClickFix popup screen

In case 2, a malicious WordPress plugin (malware called SocGholish) was planted on a website, causing it to respond with a web page containing malicious code when accessed. In addition to this malicious WordPress plugin, the same website was also planted with a PHP file for redirecting users to a fake shopping site and a web shell that can manipulate files and execute commands.

1.2.3 Targeted Attack Trends

There were 5 incidents categorized as a targeted attack. We will discuss one of them below.

1.2.3.1 Attack exploiting a vulnerability (CVE-2025-22457) in Ivanti Connect Secure

During this quarter, JPCERT/CC received a number of reports on being subjected to an attack exploiting a vulnerability (CVE-2025-22457) in Ivanti Connect Secure. All reported attacks had a backdoor called SPAWNSLOTH, SPAWNSNARE, or SPAWNCHIMERA installed in Ivanti Connect Secure, and are believed to be perpetrated by a hacker group called UNC5221, which is said to be linked to China. In some of these attacks, evidence of network infiltration has been confirmed, such as a breach of Active Directory and the use of Cobalt Strike to penetrate multiple devices.

1.2.4 Other Incident Trends

The number of malware sites reported in this quarter was 28. This was a 22% increase from 23 in the previous quarter.

The number of scans reported in this quarter was 240. This was a 6% decrease from 256 in the previous quarter. The top 10 ports that the scans targeted are listed in Table 1.4. Ports targeted frequently were Telnet (23/TCP), SSH (22/TCP), HTTP (80/TCP), and 88/TCP.

There were 484 incidents categorized as others. This was a 12% increase from 433 in the previous quarter.

Table 1.4 Top 10 ports by number of scans

Port	Apr	May	Jun	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

1.3 Incident Handling Case Examples

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

1.3.1 Notification of human-operated ransomware attacks to domestic organizations

JPCERT/CC received reports of human-operated ransomware attacks (e.g., SafePay, BlackLock) from a number of affected organizations again this quarter.

There were also a number of reports from overseas security organizations on possible ransomware attacks against the overseas group companies of Japanese companies. JPCERT/CC shared this information with the security personnel of the Japanese companies concerned and asked them to investigate the matter and take necessary steps. As a result, the notified companies were able to remove the backdoor before any damage was done from a ransomware attack, preventing the spread of damage.

Chapter 2

Analysis and Provision of Threat Intelligence

To prevent the occurrence and spread of damage caused by incidents and the like, JPCERT/CC collects and analyzes vulnerability information, threat intelligence, security information, etc. Based on the analysis, when it determines that the likelihood of occurrence or spread of damage due to incidents has increased, it provides alerts such as "Security Alerts" and "Early Warning Information," as well as information for incident response and countermeasures.

2.1 Information Collection and Analysis

The information JPCERT/CC collects and analyzes includes not only information it gathers itself, but also information received from related organizations in Japan and abroad, including CSIRTs of various regions and organizations and other relevant bodies. Based on these, we analyze information such as vulnerabilities, attack techniques, and malware used in cyberattacks that could lead to the occurrence or spread of incidents.

In addition, we collect feedback from organizations on the information provided by JPCERT/CC and use it to understand the domestic impact and to further analyze information. In particular, feedback from organizations via the portal site "CISTA (Collective Intelligence Station for Trusted Advocates)" (see 2.3) that provides Early Warning Information and the like is being effectively utilized, including dissemination to other organizations.

Among the information collected, feedback received, or information analyzed this quarter, we present notable items.

2.1.1 Stack-based buffer overflow vulnerability in Ivanti Connect Secure (CVE-2025-22457)

On April 4, 2025, Ivanti published an advisory[*1] on a stack-based buffer overflow vulnerability (CVE-2025-22457) in Ivanti Connect Secure, Policy Secure, and the ZTA Gateway. On the same day, Mandiant published[*2] a report on attacks exploiting this vulnerability. Because systems believed to be affected by this vulnerability are widely used domestically, and because it became apparent that attacks exploiting this vulnerability could occur in Japan, JPCERT/CC immediately published an Alert[*3] and provided information on addressing the vulnerability and investigating possible compromise. Furthermore, JPCERT/CC collaborated with organizations in Japan and overseas and sent individual notifications to the administrative organizations of systems that could be affected by this vulnerability and systems that may already have been attacked exploiting this vulnerability, to prevent or minimize damage. Subsequently, during communications with organizations that may have been attacked, we confirmed cases where the output results of the integrity check tool provided by Ivanti were tampered with, and cases where an inadequate understanding of the tool's specifications at user organizations resulted in failure to take appropriate action. In light of these, we updated the Alert on April 30, 2025, and called for renewed vigilance.

2.1.2 Stack-based buffer overflow vulnerability in Active! mail (CVE-2025-42599)

On April 18, 2025, Qualitia published[*4] a notice regarding a stack-based buffer overflow vulnerability in Active! mail. Prior to publication, the company had reported this vulnerability to JPCERT/CC, and upon receiving it, JPCERT/CC proceeded with coordination and published vulnerability information on JVN on April 18, 2025 (JVN#22348866 Stack-based buffer overflow vulnerability in Active! mail)[*5]. For details, please refer to "Chapter Section 4 Coordination and Distribution of Vulnerability-Related Information: Status of Handling Vulnerability-Related Information." Also, because attacks exploiting this vulnerability had already been confirmed, JPCERT/CC published an Alert[*6] on the same day. Based on a report from the vulnerability discoverer, we urged those using products and services affected by this vulnerability to apply countermeasures and investigate possible compromise, providing examples such as inspection and defense methods when operating a

[*1] "April Security Advisory Ivanti Connect Secure, Policy Secure & ZTA Gateways (CVE-2025-22457)". Ivanti. https://forums.ivanti.com/s/article/April-Security-Advisory-Ivanti-Connect-Secure-Policy-Secure-ZTA-Gateways-CVE-2025-22457, (2025-04-03).

[*2] "Suspected China-Nexus Threat Actor Actively Exploiting Critical Ivanti Connect Secure Vulnerability (CVE-2025-22457)". Mandiant. https://cloud.google.com/blog/topics/threat-intelligence/china-nexus-exploiting-critical-ivanti-vulnerability, (2025-04-04).

[*3] "Advisory on vulnerabilities in Ivanti Connect Secure, etc. (CVE-2025-22457)". JPCERT/CC. https://www.jpcert.or.jp/at/2025/at250008.html, (2025-04-04).

[*4] "Important Notice Regarding a Vulnerability in Active! mail 6". Qualitia. https://www.qualitia.com/jp/news/2025/04/18_1030.html, (2025-04-18).

[*5] "JVN#22348866 Active! mail vulnerable to stack-based buffer overflow". JVN. https://jvn.jp/jp/JVN22348866/, (2025-04-18).

[*6] "Advisory on a stack-based buffer overflow vulnerability in Active! mail". JPCERT/CC. https://www.jpcert.or.jp/at/2025/at250010.html, (2025-04-18).

web application firewall (WAF) as ways to mitigate the impact of this vulnerability. Furthermore, we distributed information on attack indicators shared by organizations that had suffered attacks exploiting this vulnerability to CISTA service users within the same month as indicator information.

2.1.3 Vulnerabilities in Ivanti Endpoint Manager Mobile (EPMM) (CVE-2025-4427, CVE-2025-4428)

On May 13, 2025, Ivanti published a security advisory*7 on vulnerabilities in Ivanti Endpoint Manager Mobile (EPMM). The product contains an authentication bypass vulnerability (CVE-2025-4427) and an arbitrary code execution vulnerability (CVE-2025-4428), and combining these vulnerabilities could allow arbitrary code execution without authentication. According to Ivanti, exploitation of the vulnerabilities has been confirmed at a very small number of user organizations. Since JPCERT/CC had confirmed that products potentially affected by these vulnerabilities were operating in Japan, we published an Alert*8 on May 14, 2025, and subsequently provided information to organizations believed to be using the product.

2.2 Information Provided on the Website

JPCERT/CC publishes information such as "Security Alerts," "CyberNewsFlash," and "Weekly Report" on its website. We provide an RSS feed, and some information is also delivered via email to mailing list subscribers (about 42,000 as of the end of this quarter).

2.2.1 Security Alerts

When serious vulnerabilities with broad impact are published, we issue an Advisory to widely call on users to take countermeasures.

- JPCERT/CC Security Alerts
  https://www.jpcert.or.jp/at/

This quarter, we published 7 items and updated 2 items.

- 2025-04-04 Advisory on vulnerabilities in Ivanti Connect Secure, etc. (CVE-2025-22457) (Published)
- 2025-04-09 Advisory on Microsoft Security Updates for April 2025 (Published)
- 2025-04-18 Advisory on a stack-based buffer overflow vulnerability in Active! mail (Published)

*7 "Security Advisory Ivanti Endpoint Manager Mobile (EPMM) May 2025 (CVE-2025-4427 and CVE-2025-4428)". Ivanti. https://forums.ivanti.com/s/article/Security-Advisory-Ivanti-Endpoint-Manager-Mobile-EPMM, (2025-05-13).

*8 "Alert regarding vulnerabilities in Ivanti Endpoint Manager Mobile (EPMM) (CVE-2025-4427, CVE-2025-4428)". JPCERT/CC. https://www.jpcert.or.jp/at/2025/at250011.html, (2025-05-14).

- 2025-04-30 Advisory on vulnerabilities in Ivanti Connect Secure, etc. (CVE-2025-22457) (Updated)
- 2025-05-09 Advisory on an authentication bypass vulnerability in Fortinet FortiOS and FortiProxy (CVE-2024-55591) (Updated)
- 2025-05-14 Advisory on Microsoft Security Updates for May 2025 (Published)
- 2025-05-14 Advisory on vulnerabilities in Ivanti Endpoint Manager Mobile (EPMM) (CVE-2025-4427, CVE-2025-4428) (Published)
- 2025-06-11 Advisory on Microsoft Security Updates for June 2025 (Published)
- 2025-06-11 Advisory on vulnerabilities in Adobe Acrobat and Reader (APSB25-57) (Published)

2.2.2 CyberNewsFlash

JPCERT/CC may publish information that does not meet the criteria for an Advisory at the time of publication, such as information on vulnerabilities, malware, and cyberattacks, as a CyberNewsFlash.

- JPCERT/CC CyberNewsFlash
  https://www.jpcert.or.jp/newsflash/

This quarter, we published 3 items.

- 2025-04-17 Observation of communications from ASUS WiFi routers running AiCloud
- 2025-05-12 On attacks combining multiple vulnerabilities (CVE-2023-44221, CVE-2024-38475) in SonicWall SMA 100 Series
- 2025-05-22 On a vulnerability in ISC BIND 9 (May 2025)

2.2.3 Weekly Report

We compile a summary of the security-related information collected by JPCERT/CC that we deem important and, in principle, publish it every Wednesday (the third business day of each week) as a Weekly Report. This quarter, we published 12 issues and provided a total of 94 pieces of security information.

- JPCERT/CC Weekly Report
  https://www.jpcert.or.jp/wr/

2.3 Information sharing via CISTA

JPCERT/CC operates CISTA, a registration-based information-sharing platform. Those wishing to receive Early Warning Information register, and we share information with approximately 1,260 organizations, including information security departments supporting critical infrastructure and in-house CSIRTs. For details on the framework of Early Warning Information, please refer to the following web page.

- Early Warning Information
  https://www.jpcert.or.jp/wwinfo/

In CISTA, recipient organizations can provide feedback or replies to information provided by JPCERT/CC. Feedback and replies received are utilized and shared back with other organizations, in accordance with the permitted sharing scope.

2.3.1 Early Warning Information

Among the collected vulnerability and threat intelligence, items judged likely to have a significant impact on critical information infrastructure, etc., and that should be shared early with organizations providing critical infrastructure are provided as Early Warning Information. This quarter, we issued 1 item.

2.3.2 Analyst Note

Among the collected vulnerability and threat intelligence, items that JPCERT/CC considers noteworthy are compiled daily and provided as Analyst Note. This quarter, we issued 62 items.

2.3.3 Individually Provided Information

From the collected information, we individually provide vulnerability and threat information that is considered to affect specific organizations. For example, we provide information to organizations that operate Vulnerable Hosts, such as hosts where countermeasures for serious vulnerabilities have not been applied, or hosts that may already have unauthorized programs installed, be defaced, or have credentials stolen due to exploitation. If individual information cannot be provided via CISTA to the target organization, we may notify the contact registered in JPNIC WHOIS, or request notification via the ISP or maintenance vendor. This quarter, we provided 65 items. We provided information to organizations managing hosts affected by the vulnerabilities in Ivanti Connect Secure (CVE-2025-22457), Active! mail (CVE-2025-42599), and Ivanti Endpoint Manager Mobile (EPMM) (CVE-2025-4427, CVE-2025-4428), among others.

Chapter 3

Observation and analysis of reconnaissance and attack activities on the Internet

JPCERT/CC has developed observation sensors that collect packets sent to an unspecified large number of hosts and, by using hosting services and other means, has deployed multiple sensors domestically and internationally to build and operate the Internet threat monitoring system "TSUBAME." Packets sent to the sensors are considered to be attempts to probe specific devices or service functions. JPCERT/CC continuously collects packets observed by the sensors and analyzes them against vulnerability information, malware and attack tool information, and more. These analyses can reveal attack activities over the Internet and preparatory activities for attacks, enabling rapid identification of global attack activities.

3.1 Observation using the Internet threat monitoring system "TSUBAME"

TSUBAME records TCP, UDP, and ICMP packets among those that reach the sensors from the Internet. Unlike honeypots, the sensors do not respond to incoming packets. TSUBAME observes traffic that poses security threats, such as worm propagation and scans for weaknesses. For more information on TSUBAME, please see the following web page.

- TSUBAME (Internet threat monitoring system)
  https://www.jpcert.or.jp/tsubame/index.html

3.1.1 Utilizing TSUBAME observation data

To help system administrators at various organizations with incident response and countermeasures, JPCERT/CC provides observation data obtained through TSUBAME. This quarter, in addition to providing individualized information based on observation data, we published the Internet Threat Monitoring Report and the blog "TSUBAME Report Overflow," which introduce observation trends

and noteworthy phenomena. The blog covers analyses that could not be fully included in the report and distinctive events that occurred during the period. In "TSUBAME Report Overflow (January–March 2025)," we reviewed incident examples related to Japan from last fiscal year's observations and presented findings on the observation status of reconnaissance packets characteristic of Mirai and on source characteristics.

- JPCERT/CC Internet Threat Monitoring Report [January 1, 2025–March 31, 2025]
  https://www.jpcert.or.jp/tsubame/report/report202501-03.html
- TSUBAME Report Overflow (January–March 2025)
  https://blogs.jpcert.or.jp/ja/2025/06/tsubame-overflow20250103.html

In addition, because multiple cases have been observed in which the sources of reconnaissance packets seen by TSUBAME were network cameras, we provided observation data and other information to the Japan Security Systems Association and cooperated in the creation of the "Security Camera System Network Construction Guide II (Supplement)" (防犯カメラシステムネットワーク構築ガイドII別冊).

3.1.2 TSUBAME observation trends

Below is a breakdown by destination port of the packets received by TSUBAME sensors in Japan this quarter. Please use it as a reference when analyzing the trends of packets reaching your organization's network.

For the destination ports that ranked in the top 10 by total packet count this quarter when packets observed by sensors installed in Japan are grouped by destination port, we show daily increases and decreases in packet counts, split into ranks 1–5 and 6–10 (Figure 3.1, 3.2).

We also show trends over the past year (July 1, 2024–June 30, 2025) for destination ports ranked 1–5 and 6–10 by packet count (Figure 3.3, 3.4).

The most frequently observed packets this quarter were communications to 23/TCP (Telnet), with a sharp increase around April 5, 2025. 80/TCP ranked second and 443/TCP third, swapping ranks with 8728/TCP, which moved to fourth compared to the previous quarter. Reconnaissance packets targeting web ports are increasing. For 22/TCP in fifth place, while there were temporary fluctuations, there was no significant change.

3.2 Honeypot operation and analysis

JPCERT/CC deploys low-interaction honeypots on the Internet that record communications to services such as HTTP and HTTPS, collects various communications sent by attackers, and analyzes attack activities together with TSUBAME observation results.

We participated in the Honeynet Project Annual Workshop 2025, held from June 2 to June 4, 2025,

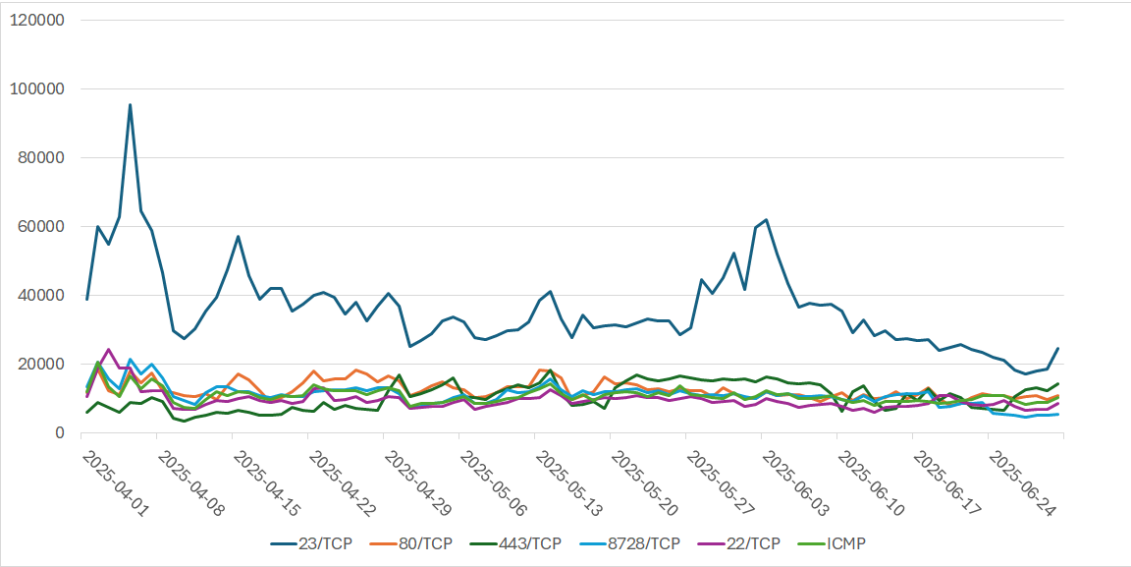

Figure 3.1 Packet counts for destination ports ranked 1–5 observed by TSUBAME (April 1, 2025 – June 30, 2025)

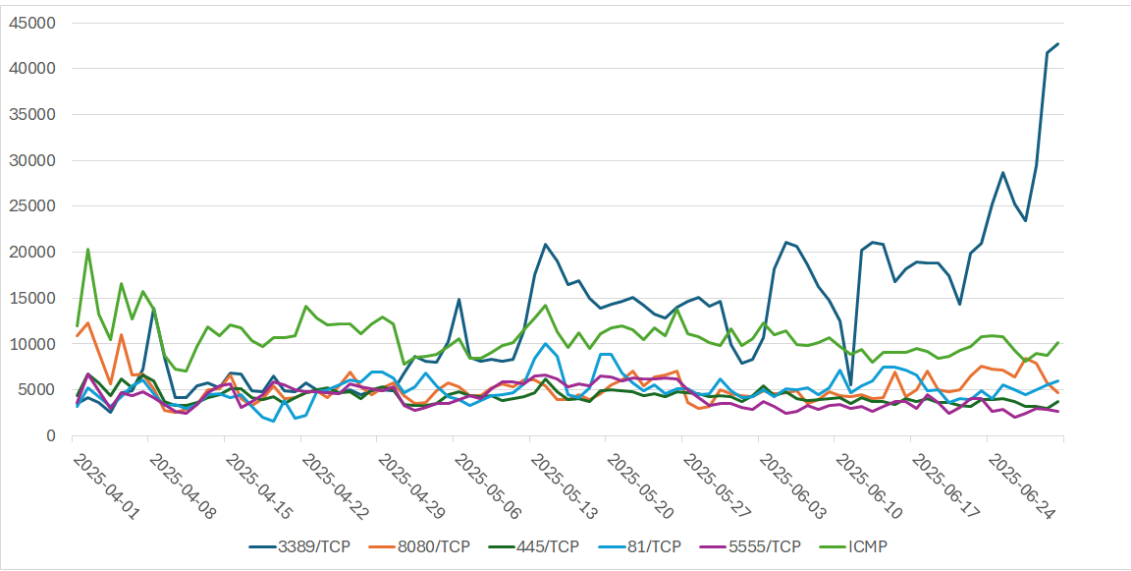

Figure 3.2 Packet counts for destination ports ranked 6–10 observed by TSUBAME (April 1, 2025 – June 30, 2025)

where developers and operators of honeypots gather, to collect information and exchange views. For details on the Honeynet Project Annual Workshop 2025, please refer to the following web page.

- The Honeynet Project Annual Workshop 2025
  https://prague2025.honeynet.org/

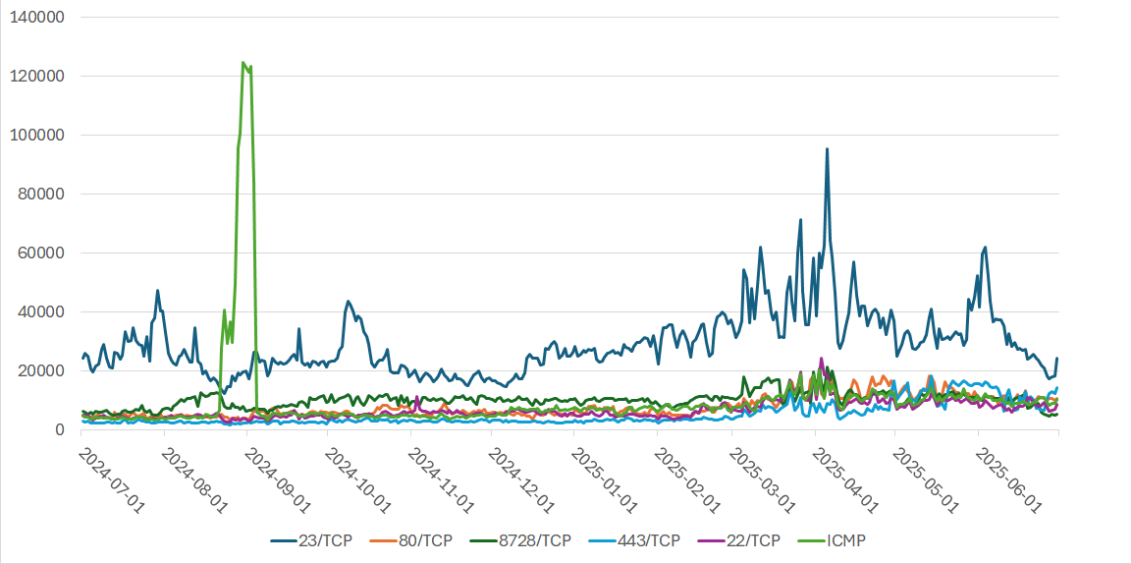

Figure 3.3 Packet counts for destination ports ranked 1–5 observed by TSUBAME (July 1, 2024 – June 30, 2025)

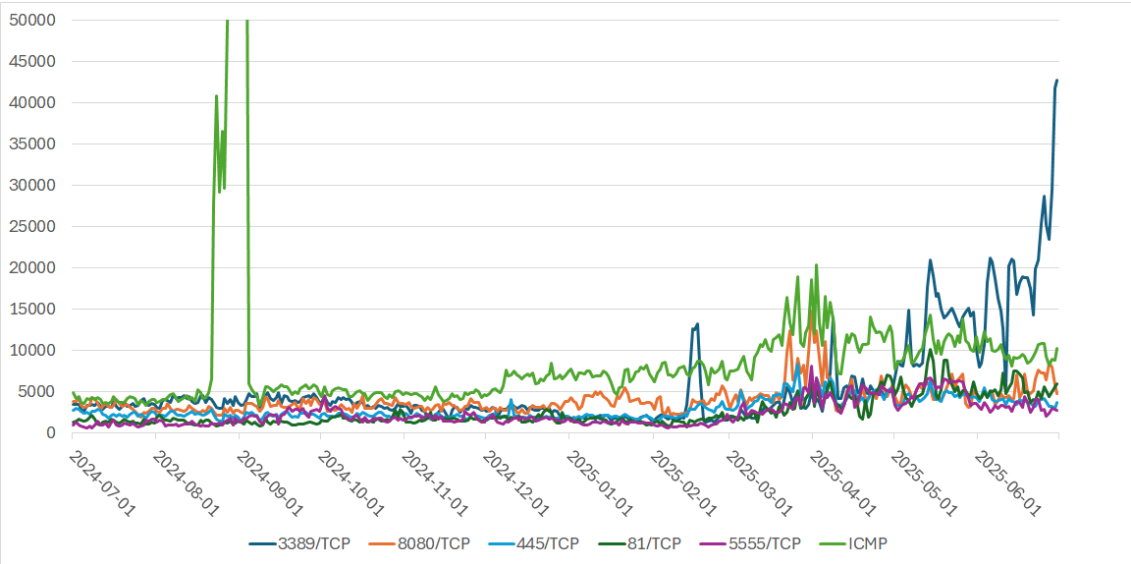

Figure 3.4 Packet counts for destination ports ranked 6–10 observed by TSUBAME (July 1, 2024 – June 30, 2025)

Chapter 4

Coordination and dissemination of vulnerability-related information

With the aim of ensuring the safety of software product users, JPCERT/CC promotes countermeasures by product developers by disclosing discovered vulnerability information to appropriate parties in a timely manner, and raises broad awareness by publishing vulnerability information together with mitigation information prepared by product developers through JVN (Japan Vulnerability Notes), a vulnerability information portal jointly operated with the Information-technology Promotion Agency, Japan (IPA). Furthermore, we are working on promoting secure coding to prevent the introduction of vulnerabilities, as well as addressing vulnerabilities in control systems.

4.1 Handling status of vulnerability-related information

4.1.1 Handling of vulnerability-related information at JPCERT/CC

At JPCERT/CC, for vulnerability-related information received, we identify the product developers related to the vulnerability in question, contact the appropriate points of contact for the vulnerability-related information, coordinate verification and remediation by the product developers, and publish vulnerability information, etc. to the public through JVN. In addition, to facilitate the international and effective circulation of published vulnerability information, within the CVE (Common Vulnerabilities and Exposures) Program (an international initiative driven by the expert community since 1999, whose mission is to identify, describe, and catalog publicly disclosed individual vulnerabilities; administered by MITRE in the United States), we serve as a Root that oversees subordinate CNAs (CVE Numbering Authorities) and also act as a CNA ourselves to assign CVE IDs.

As a “Coordination Body” based on the Ministry of Economy, Trade and Industry notification “Regulations on the Handling of Vulnerability-Related Information for Software Products, etc.” (ソフトウエア製品等の脆弱性関連情報に関する取扱規程) (Ministry of Economy, Trade and Industry Notification No. 19 of 2017; last amended by Ministry of Economy, Trade and Industry Notifica-

tion No. 93 of 2024), JPCERT/CC carries out coordination with product developers. Activities as a Coordination Body are conducted in close collaboration with IPA, the "reporting body" for vulnerability information, in accordance with the "Information Security Early Warning Partnership Guideline" (hereinafter, "Partnership Guideline") based on these regulations.

We also conduct international coordination with overseas coordination organizations such as CERT/CC, CISA, NCSC-NL, and NCSC-FI, and handle reports and coordination requests from both domestic and overseas sources.

4.1.2 Vulnerability information and response status published on Japan Vulnerability Notes (JVN)

The vulnerability information published on JVN is classified into the following three categories.

- Vulnerability-related information reported based on the Partnership Guideline (assigned an identifier in the format "JVN#" followed by 8 digits; e.g., JVN#12345678)
- Vulnerability information received directly from reporters, product developers, overseas coordination bodies, etc., without going through the Partnership Guideline (assigned an identifier in the format "JVNVU#" followed by 8 digits; e.g., JVNVU#12345678)
- Information that goes beyond vulnerabilities in individual products, such as issues in communication protocols or programming language standards (assigned an identifier in the format "JVNTA#" followed by 8 digits; e.g., JVNTA#12345678)

This quarter, 124 vulnerability information items were published on JVN, bringing the cumulative total to 5,859 (Figure 4.1).

For individual vulnerability information published this quarter, please refer to the following web page.

- JVN (Japan Vulnerability Notes)
  https://jvn.jp/

The breakdown of the number of vulnerability information items that were published this quarter is as follows.

- Those concerning vulnerability information reported based on the Partnership Guideline: 23
- Those concerning vulnerability information based on international coordination or our own coordination: 101
- Those concerning technical information related to vulnerability information: 0

Note that the quarterly status of reports concerning vulnerability-related information based on the Partnership Guideline can be found on the following web page.

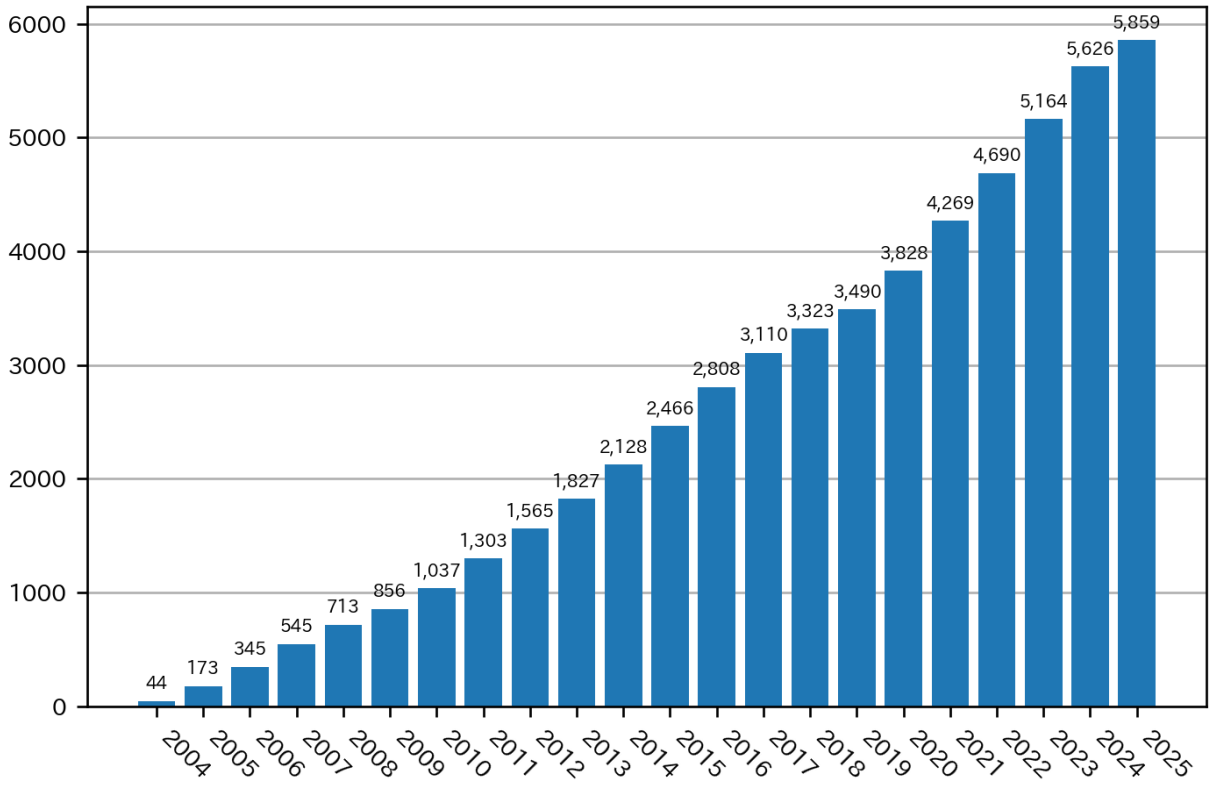

Figure 4.1 Cumulative number of JVN publications

- Information-technology Promotion Agency, Japan (IPA): Status of reports concerning vulnerability-related information for software, etc. (ソフトウェア等の脆弱性関連情報に関する届出状況)
  https://www.ipa.go.jp/security/reports/vuln/software/index.html

Among the vulnerabilities published this quarter, we highlight notable cases reported based on the Partnership Guideline and those handled through international or our own coordination.

4.1.2.1 Notable vulnerabilities reported based on the Partnership Guideline

- JVN#22348866
  Stack-based buffer overflow vulnerability in Active! mail
  https://jvn.jp/jp/JVN22348866/

This is an advisory regarding a vulnerability in "Active! mail," a business webmail product provided by Qualitia. When a crafted request is sent by a remote third party, this vulnerability may allow arbitrary code execution without authentication, and exploitation could have serious impact on users. Along with the vulnerability information, the product developer reported to JPCERT/CC that attacks exploiting the vulnerability had been confirmed. When there is information indicating exploitation, in addition to coordination toward publishing an advisory on JVN, JPCERT/CC

responds broadly by, for example, issuing alerts and providing information for incident response and countermeasures. In this advisory, to draw users' attention, we marked the title "Urgent" and noted in the body that attacks were being observed. After publishing the advisory, we also issued an alert, urging users to take swift action. For details on the alert related to this case, see Section 2.1.2.

4.1.2.2 Notable vulnerabilities handled through international or our own coordination

- JVNVU#93701955
  Multiple out-of-bounds write vulnerabilities in certain printer drivers for Canon production/office/small office multifunction printers and laser beam printers
  https://jvn.jp/vu/JVNVU93701955/

This is an advisory regarding vulnerabilities in Canon printer drivers such as LIPSLX, LIPS4, PS3, PCL6, and CARPS2, which are incorporated into both Japan-market and overseas-market products. Canon first published information about this vulnerability on the Common Vulnerabilities and Exposures site (https://www.cve.org/), and after confirming this, JPCERT/CC worked with the company to prepare a JVN advisory to promote the circulation of the vulnerability information. Because affected products have different product names and model numbers depending on the region, the company coordinated with its affiliates in Japan, the U.S., and Europe to prepare and publish region-specific advisories. For products with broad global distribution, product names and model numbers may differ by region. For vulnerabilities in such products, coordination with regional affiliates may be undertaken so that advisories can be issued for each region. In addition, when multiple advisories are issued for a single vulnerability, coordination is needed to ensure there are no differences in content such as countermeasures and to align publication timing. Even in cases where the regions and stakeholders involved are diverse, JPCERT/CC conducts Coordinated Vulnerability Disclosure (CVD) through close and friendly collaboration, pays careful attention to the timing and content of publications, and strives to ensure the security of product users.

4.1.3 Start of evaluation using the Common Vulnerability Scoring System "CVSS v4.0"

In November 2023, FIRST released CVSS v4.0. As a major update from CVSS v3.1, CVSS v4.0 includes greater granularity in the Base Metrics and improvements to reduce ambiguity in the evaluation items. On JVN, CVSS v2.0 was posted from April 1, 2014 (posting ended on March 31, 2024), and CVSS v3.0/v3.1 has been posted since December 1, 2015. At JPCERT/CC, we have been preparing for posting CVSS v4.0 on JVN by considering how to include CVSS v4.0 in JVN advisories and conducting study sessions aimed at acquiring CVSS v4.0 evaluation skills. Then, starting April 21, 2025, we began including CVSS v4.0 in newly published JVN advisories.

- Notice of adoption of evaluation using CVSS v4 (2025-04-14)
  https://jvn.jp/nav/info2025041471.html

4.1.4 Handling uncontactable developers

For vulnerabilities reported under the Partnership Guidelines, if the product developer cannot be reached, there are cases where we handle them in accordance with the procedures (announced in May 2014; guideline revision) for publishing cases involving uncontactable developers through consultation with the Publication Review Committee, etc. Based on these procedures, JPCERT/CC publishes on JVN the "List of Uncontactable Developers," which broadly seeks leads for contacting the relevant product developers, and the "Japan Vulnerability Notes JP (Uncontactable) List," which informs product users of vulnerabilities deemed appropriate for publication by the Publication Review Committee. In this quarter, the number of new publications for both the "List of Uncontactable Developers" and the "Japan Vulnerability Notes JP (Uncontactable) List" is 0.

- List of Uncontactable Developers
  https://jvn.jp/reply/
- Japan Vulnerability Notes JP (Uncontactable) List
  https://jvn.jp/adj/

4.1.5 Activities as a CNA and as a Root

JPCERT/CC participates in the CVE Program to facilitate the international distribution of vulnerability information, acting as a CNA to assign CVE IDs and as a Root to conduct activities scoped to domestic product developers.

Since May 2008, except for cases where another CNA assigned the ID, JPCERT/CC has assigned CVE IDs to vulnerability information published on JVN. In this quarter, CVE IDs were assigned to 64 vulnerabilities.

For details on CNA and CVE, please refer to the following web page.

- CNA (CVE Numbering Authority)
  https://www.jpcert.or.jp/vh/cna.html
- Overview About the CVE Program
  https://www.cve.org/About/Overview

4.2 Developing a domestic vulnerability information distribution framework in Japan

JPCERT/CC is developing a framework for the distribution of vulnerability information. For details, please refer to the following web pages.

- Vulnerability Information Handling Framework
  https://www.meti.go.jp/policy/netsecurity/vulinfo.html

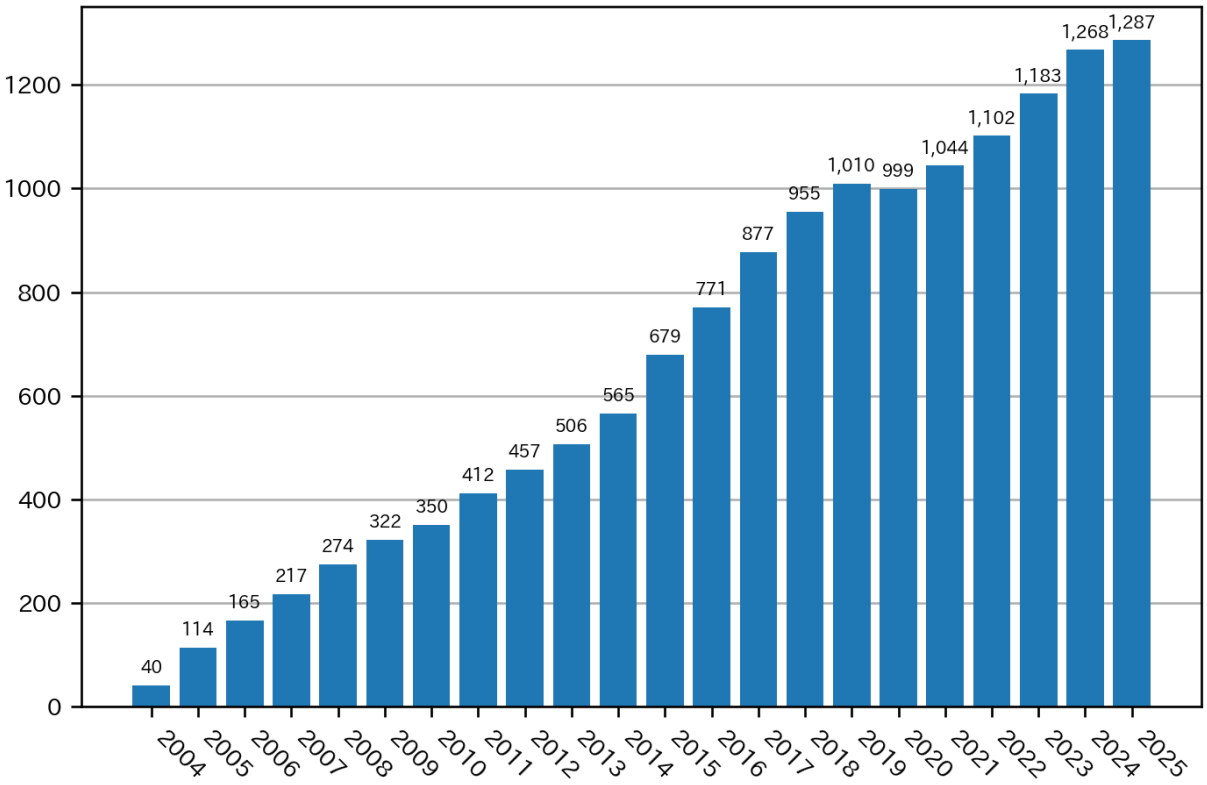

Figure 4.2 Number of Registered Product Developers

- What is Vulnerability Information Handling?
  https://www.jpcert.or.jp/vh/
- Information Security Early Warning Partnership Guidelines (2024 edition)
  https://www.jpcert.or.jp/vh/partnership_guideline2024.pdf
- JPCERT/CC Vulnerability Information Handling Guidelines (2019 edition)
  https://www.jpcert.or.jp/vh/vul-guideline2019.pdf

4.2.1 Collaboration with product developers in Japan

As a coordination organization, JPCERT/CC maintains a list of product developers that are recipients of vulnerability information. We ask product developers to register in the product developer list. The number of registered product developers as of the end of this quarter is 1,287 (Figure 4.2). For details on registration, please refer to the following web page.

- Product Developer Registration
  https://www.jpcert.or.jp/vh/register.html

Chapter 5

Domestic Collaboration Activities

To smoothly carry out the coordination tasks described in the previous chapters, we may need the cooperation of each organization's CSIRT and industry associations engaged in addressing cybersecurity challenges. To prepare for such cases, JPCERT/CC strives in normal times to share information and awareness about the security situation with those organizations and works to build an environment that enables smooth collaboration in emergencies.

5.1 Collaboration with industry associations and communities

We participate in gatherings hosted by organizations such as ISACs and CEPTOARs in various industries engaged in cybersecurity initiatives, as well as industry associations and academic societies, where we exchange views and give presentations, among others. This quarter, we conducted the following activities.

5.1.1 SICE/JEITA/JEMIMA Joint Working Group on Security Research

We participated in the Joint Working Group on Security Research, which is regularly held by SICE (The Society of Instrument and Control Engineers), JEITA (Japan Electronics and Information Technology Industries Association), and JEMIMA (Japan Electric Measuring Instruments Manufacturers' Association), and exchanged opinions with experts on control system security.

5.1.2 CEPTOAR Council Steering Committee

JPCERT/CC participates in the activities of the CEPTOAR Council, supports working group activities and provides information, and jointly with the National center of Incident readiness and Strategy for Cybersecurity (NISC) [*1] supports the secretariat of the CEPTOAR Council. In this quarter, at the 80th CEPTOAR Council Steering Committee held on June 2, 2025, we shared information on the status of attack activities exploiting vulnerabilities in Ivanti Connect Secure and

[*1] Reorganized into the National Cybersecurity Office (NCO) on July 1, 2025

Active! mail.

5.2 Strengthening collaboration and establishing an environment for information exchange with domestic stakeholders

5.2.1 Promoting collaboration with early warning information recipients

For organizations registered on the CISTA portal site, in addition to providing early warning information, we create opportunities for information sharing and opinion exchange. We promote interaction among organizations by holding in-person meetings and encourage active dialogue, including inviting talks from representatives of registered organizations. Note that this quarter, 10 new organizations registered with CISTA.

5.2.2 Working group for control system security personnel in the manufacturing industry

JPCERT/CC hosts a working group of control system security personnel, primarily from the manufacturing sector, to discuss issues. In this group, JPCERT/CC and practitioners from participating organizations collaborate to conduct practical examinations of common issues related to control system security.

As of the end of this quarter, 34 organizations are participating.

5.3 Provision of information and tools

5.3.1 Mailing list for providing control system security information

We had been distributing ICS Security Notes via a mailing list for control system security information, but due to the termination of that service described later, we discontinued the mailing list at the end of April 2025.

Regarding the provision of information on control system security, we will henceforth focus on initiatives utilizing JPCERT/CC's website and other channels.

5.3.2 JPCERT/CC ICS Security Notes

JPCERT/CC ICS Security Notes was a quarterly distribution that provided overseas cases and standardization trends along with announcements from JPCERT/CC. From among the public information on control system security collected by JPCERT/CC, we selected items warranting particular attention and compiled them concisely so readers could understand developments during the target period.

The ICS Security Notes provided this quarter are as follows.

- 2025-04-15 JPCERT/CC ICS Security Notes FY2024_#Q4

As domestic organizations have made a certain degree of progress in collecting public information related to control system security, we determined that ICS Security Notes had fulfilled its role and ended the service with the above distribution. Going forward, through the "Working group for control system security personnel in the manufacturing industry" and the "Control System Security Conference," among others, we will focus on initiatives that lead to more practical problem-solving.

5.3.3 Provision of a self-assessment tool for control system security

JPCERT/CC provides free, easy-to-use security self-assessment tools—Japan SSAT (SCADA Self Assessment Tool: application required) and J-CLICS (control system security self-assessment tool)—with the aim of extracting security issues related to the construction and operation of control systems and enabling well-balanced security measures.

- Japan SSAT (SCADA Self Assessment Tool)
  https://www.jpcert.or.jp/ics/ssat.html
- J-CLICS STEP1/STEP2 (ICS Security Self-Assessment Tool)
  https://www.jpcert.or.jp/ics/jclics.html
- J-CLICS Attack Path Countermeasures Edition (ICS Security Self-Assessment Tool)
  https://www.jpcert.or.jp/ics/jclics-attack-path-countermeasures.html

Chapter 6

International Collaboration Activities

Many of the incidents JPCERT/CC handles require information sharing and collaboration with overseas CSIRTs, ISPs, and government agencies. Therefore, even before incidents occur, JPCERT/CC identifies trusted counterparts in each country and builds trust relationships to enable mutual cooperation when needed. In this chapter, we highlight notable outcomes of such international collaboration activities.

6.1 Support for Building and Operating Overseas CSIRTs

To enhance incident response coordination capabilities of overseas National CSIRTs and others, JPCERT/CC provides support for CSIRT establishment and operations through training sessions and presentations at events.

6.2 International Collaboration among CSIRTs

We actively participate in multilateral CSIRT collaboration frameworks, taking leading roles in APCERT and FIRST, among others.

6.2.1 APCERT (Asia Pacific Computer Emergency Response Team)

APCERT is a CSIRT community in the Asia-Pacific region launched in February 2003. Since its inception, JPCERT/CC has continuously been elected to the Steering Committee and also serves as its Secretariat.

For details on APCERT and JPCERT/CC's role within APCERT, please refer to the following web page.

- JPCERT/CC within APCERT
  https://www.jpcert.or.jp/english/apcert/

6.2.1.1 Holding of the APCERT Steering Committee Meeting

The APCERT Steering Committee held a teleconference on May 22, 2025, to discuss APCERT's operational policies and related matters. JPCERT/CC participated as a Steering Committee member and, as the Secretariat, supported the operation of the meeting.

6.2.2 FIRST (Forum of Incident Response and Security Teams)

Since joining in 1998, JPCERT/CC has actively participated in FIRST activities. Since June 2021, Yukako Uchida, Manager of the Global Coordination Division, has served on the FIRST Board of Directors. This quarter, in addition to the monthly online board meetings, we also attended an in-person board meeting held in Copenhagen in June 2025. For details about FIRST, please refer to the following web page.

- FIRST
  https://www.first.org/
- FIRST.Org, Inc., Board of Directors
  https://www.first.org/about/organization/directors

6.2.2.1 Participation in the 37th FIRST Annual Conference

The 37th FIRST Annual Conference was held in Copenhagen, Denmark, from June 22, 2025 to June 27, 2025. This conference is held annually to exchange the latest trends in the prevention, response, and technical analysis of cyber incidents and to strengthen collaboration among incident response teams. This year, under the theme "Fortresses of the Future: Building Bridges not Walls," a wide variety of topics were covered, and 1,055 participants from 103 countries attended on-site. At this event, JPCERT/CC delivered a talk titled "Establishing a Global Community of Practice on Coordinated Vulnerability Disclosure (CVD)" (Figure 6.1) and, together with a representative from U.S. CISA, presented on initiatives within the international community related to vulnerability information distribution launched under CISA's leadership.

In addition, we used this opportunity to exchange views individually with National CSIRTs and product vendors' CSIRTs from around the world. Through participation in such gatherings, we will continue to promote information sharing across regions and foster trust relationships, thereby facilitating smoother international incident response coordination.

For more details on the 37th FIRST Annual Conference, please refer to the following web page.

- 37th Annual FIRST Conference
  https://www.first.org/conference/2025/
- FIRSTCON25 Delivers Global Collaboration and Groundbreaking Cybersecurity Initiatives
  https://www.first.org/newsroom/releases/20250627

Figure 6.1 JPCERT/CC's presentation

6.2.2.2 Reelection to the FIRST Board of Directors

The 10 directors who form the FIRST Board of Directors, which plans and formulates FIRST activities, are elected by member organizations. Directors serve two-year terms, with half the seats up for election each year. Voting is conducted online, and on June 23, 2025, at the Annual General Meeting, the election of five directors, including Uchida, was announced. As a result, Uchida began her third term. For other Board of Directors members, please refer to the following web page.

- FIRST.Org,Inc., Board of Directors
  https://www.first.org/about/organization/directors

6.3 Participation in Other International Conferences

6.3.1 Participation in Locked Shields

From May 6 to May 9, 2025, we participated online in Locked Shields 2025, an international cyber exercise hosted by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Four JPCERT/CC staff members joined participants from the Japanese government and critical infrastructure operators as part of the Blue Team, tackling incident response as well as legal and public relations challenges.

- Locked Shields
  https://ccdcoe.org/exercises/locked-shields/

6.3.2 Participation in NatCSIRT 2025

Following the 37th FIRST Annual Conference, the National CSIRT Meeting (NatCSIRT) 2025, hosted by U.S. CERT/CC, was held in Copenhagen, Denmark. This annual meeting brings together National CSIRTs from around the world to share activity plans and challenges as their nations' incident response teams, and to present and discuss development tools, joint projects, research, and more.

For details about NatCSIRT, please refer to the following web page.

- NatCSIRT 2025
  https://resources.sei.cmu.edu/news-events/events/natcsirt/index.cfm

6.4 International Standardization Activities

Through the Information Technology Standards Commission of the Information Processing Society of Japan, we participate in some of the standardization work being considered in ISO/IEC JTC 1/SC 27 for IT security, including work items in WG3 (responsible for standards on security evaluation, testing, and specification) and revisions to standards on incident management in WG4 (responsible for standards on security controls and services).

This quarter, we continued preparing our response, including information gathering, regarding documents on methods for vulnerability information disclosure and vulnerability handling for which revisions were proposed at international meetings.

6.5 Building an International Framework for Vulnerability Coordination and Information Sharing

JPCERT/CC collaborates with overseas coordination organizations responsible for vulnerability information coordination in each region, such as U.S. CISA and CERT/CC, to work together on smooth international coordination and distribution of vulnerability information. We also participate in international community activities related to vulnerabilities, including FIRST, to build foundations for collaboration. Highlights of this quarter's activities are presented below.

6.5.1 Presentation at CVE/FIRST VulnCon 2025 & Annual CNA Summit

From April 7, 2025 to April 10, 2025, CVE/FIRST VulnCon 2025 & Annual CNA Summit, jointly hosted by the CVE Program and FIRST's PSIRT SIG, was held in Raleigh, North Carolina, USA. JPCERT/CC delivered a presentation, together with U.S. stakeholders, on the Global Community of Practice on Coordinated Vulnerability Disclosure (CVD-COP)—an international vulnerability coordinator community established in 2024 in which JPCERT/CC also participates—covering its

founding purpose and issues currently identified through this activity. For event details, please refer to the following web page.

- CVE/FIRST VulnCon 2025 & Annual CNA Summit
  https://www.first.org/conference/vulncon2025/

Chapter 7

Council of Anti-Phishing Japan Activities

The Council of Anti-Phishing Japan (hereinafter in this chapter, the "Council") is a membership organization that collects and provides information on phishing, analyzes trends, and examines technical and institutional responses. Commissioned by the Ministry of Economy, Trade and Industry, JPCERT/CC handles portions of the Council's activities, including accepting phishing-related reports and inquiries from general consumers, issuing alerts about phishing sites, and operating certain working groups.

The Council reports phishing sites received from the public to JPCERT/CC, and upon receipt, JPCERT/CC conducts coordination to take down phishing sites as part of its incident response support activities.

In addition to activities commissioned by the Ministry of Economy, Trade and Industry, the Council carries out its own initiatives for member organizations based on decisions by the Steering Committee, and JPCERT/CC, as the secretariat, also supports the implementation of these activities. Specifically, see "Section 7.2 Activities for Council of Anti-Phishing Japan Member Organizations."

In this chapter, we describe these activities during this quarter.

7.1 Operation of the Council of Anti-Phishing Japan Secretariat

7.1.1 Accepting phishing-related reports and inquiries

The number of phishing reports increased compared to the previous quarter. The trend in the number of phishing reports over the past year is shown in Figure 7.1.

By breakdown of reports, phishing impersonating "SBI Securities" was the most reported, accounting for about 17.1% of the total. This was followed by a high number of reports of phishing impersonating "Apple," accounting for about 9.6% of the total.

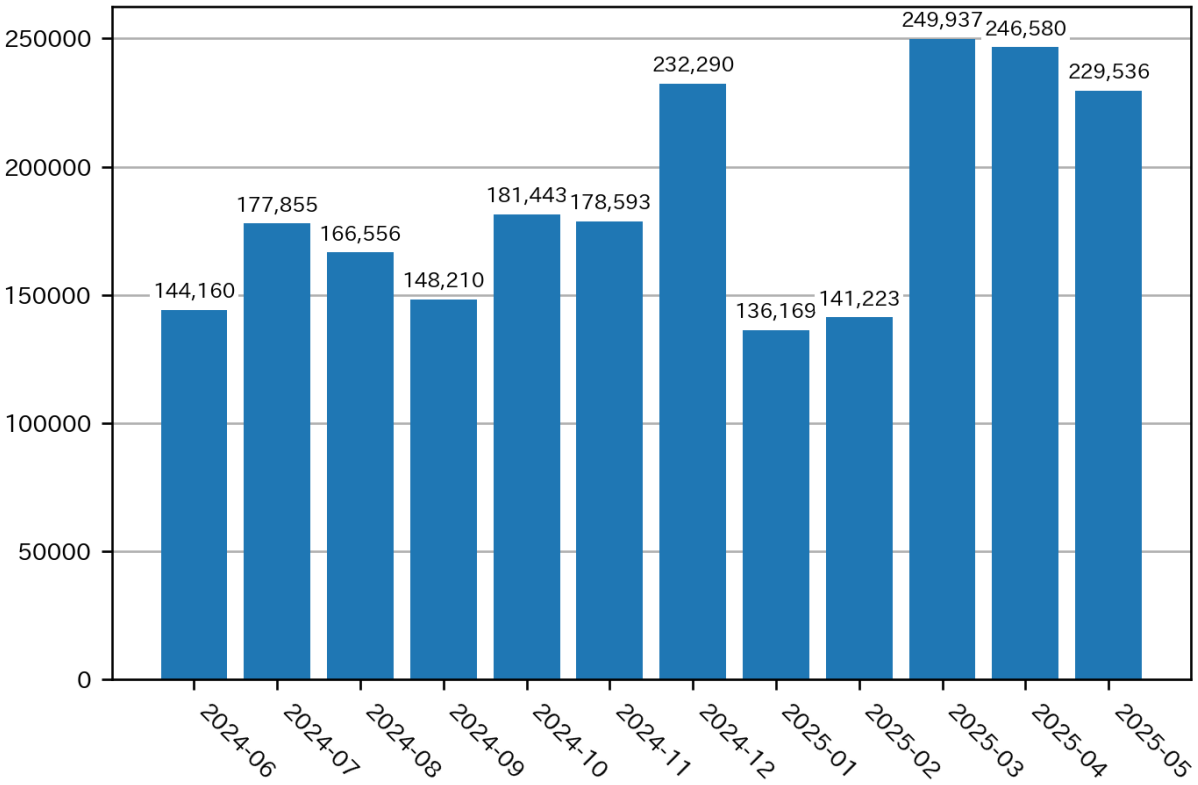

Figure 7.1 Number of phishing reports

7.1.2 Information collection/distribution

7.1.2.1 Dissemination of information on phishing trends, etc.

For phishing believed to have a wide impact related to services with many users, we post emergency notices on our website as needed to broadly raise awareness. This quarter, we issued 12 emergency phishing notices via the Council website and the members' mailing list.

- Phishing impersonating SBI Securities
- Phishing impersonating Rakuten Securities
- Phishing impersonating Nomura Securities
- Phishing impersonating Matsui Securities
- Phishing impersonating LINE
- Phishing impersonating ANA
- Phishing impersonating Tokyo Gas
- Phishing impersonating Mitsubishi UFJ Morgan Stanley Securities
- Phishing impersonating GMO CLICK Securities
- Phishing impersonating PayPay Card
- Phishing impersonating Daiwa Securities

Figure 7.2 Example of a phishing site impersonating a securities firm

- Phishing impersonating IwaiCosmo Securities

This quarter, phishing impersonating securities firms, which had continued from the previous quarter, increased significantly (Figure 7.2). There have been incidents where accounts were taken over using credentials stolen via phishing, leading to unauthorized stock trading and resulting losses, so caution is required. In addition, continuing from the previous month, there was an increase in phishing thought to be targeting the moving and travel seasons, impersonating electric and gas companies, delivery services, and airlines (Figure 7.3).

Figure 7.3 Example of a phishing site impersonating an airline

7.1.2.2 Regular reporting

We published on the Council website the number of reported phishing sites and monthly activity reports.

- Council of Anti-Phishing Japan website
  https://www.antiphishing.jp/
- 2025/03 Phishing report status
  https://www.antiphishing.jp/report/monthly/202503.html
- 2025/04 Phishing report status
  https://www.antiphishing.jp/report/monthly/202504.html
- 2025/05 Phishing report status
  https://www.antiphishing.jp/report/monthly/202505.html

7.1.2.3 Provision of phishing site URL information

We provide a list of URLs of phishing sites reported to the Council to member organizations such as vendors offering anti-phishing toolbars and antivirus software and academic institutions conducting

phishing-related research. This aims to strengthen anti-phishing products and promote related research. As of the end of this quarter, we were providing URL information to 50 organizations, and we plan to continue broad provision upon request.

7.1.2.4 Publication of Anti-Phishing Guidelines and Phishing Report

The "Technical and Institutional Study Working Group" is a working group of experts mainly from Council member organizations that creates and revises guidelines and trend reports on anti-phishing measures. On June 3, 2025, the "Anti-Phishing Guidelines FY2025 Edition," the "User Guidelines for Phishing Scam Countermeasures FY2025 Edition," and the "Phishing Report 2025," which were created and revised by the Technical and Institutional Study Working Group in FY2024, were published.

- Anti-Phishing Guidelines FY2025 Edition
  https://www.antiphishing.jp/report/guideline/antiphishing_guideline2025.html
- User Guidelines for Phishing Scam Countermeasures FY2025 Edition
  https://www.antiphishing.jp/report/guideline/consumer_guideline2025.html
- Phishing Report 2025
  https://www.antiphishing.jp/report/wg/phishing_report2025.html

7.2 Activities for Council of Anti-Phishing Japan Member Organizations

Based on decisions by the Steering Committee, JPCERT/CC, as the secretariat, supported the following independent activities for member organizations.

7.2.1 Steering Committee meetings

This quarter, the Steering Committee, which plans Council activities and decides operational policies, was held as follows.

- 127th Steering Committee (online)
  Date and time: Thursday, April 17, 2025, 16:00–18:00
- 128th Steering Committee (online)
  Date and time: Wednesday, May 21, 2025, 16:00–18:00
- 129th Steering Committee (online)
  Date and time: Thursday, June 26, 2025, 16:00–18:00

7.2.2 Support for holding working group meetings, etc.

This quarter, we supported the following Council events and meetings of working groups, etc.

- Academic Research Working Group meeting
  Date and time: Weekly on Tuesdays from April 2025 to June 2025, 9:00–9:30 (online)
- Incident Impact Sharing Working Group meeting
  Date and time: Friday, April 18, 2025, 16:00–17:00 (online)
  Date and time: Friday, May 9, 2025, 16:00–17:00 (online)
- 1st Certificate Promotion Working Group meeting
  Date and time: Friday, May 16, 2025, 16:00–17:30 (JPCERT/CC conference room + online)
- Council of Anti-Phishing Japan General Meeting FY2025
  Date and time: Tuesday, June 17, 2025, 15:00–17:00 (Essam Kanda Hall No. 2 Building)

Chapter 8

Public Relations Activities

JPCERT/CC conducts extensive public relations regarding its business outcomes to promote and raise awareness of the results. Information is distributed via the JPCERT/CC website and X (formerly Twitter), as well as through various media such as web, broadcast, and print outlets. We also disseminate information by speaking at seminars and events.

8.1 Presentations

This quarter, we gave presentations at the following seminars and events.

1. TECH+ Seminar Manufacturing × OT Security 2025 May: Preventing and Responding to Security Incidents to Protect Factories and Manufacturing Sites
   Title: How to Prepare for Cyber Threats Needed for Business Continuity — Advance Preparations Organizations and Factory Stakeholders Should Take and Where to Seek Advice in Emergencies —
   Presenter: Kazuyuki Kohno (Domestic Coordination Group ICS Security Senior Analyst)
   Organizer: Mynavi Corporation, TECH+ Seminar Operations Office
   Date of presentation: May 26, 2025
2. Cybersecurity Measures 2025 Summer
   Title: Where Do We Protect Cybersecurity? — Zero Trust and Cyber Hygiene Considered from Recent Attack Cases —
   Presenter: Hayato Sasaki (General Manager of Strategy and Early Warning Group Manager, Threat Analyst)
   Organizer: SB Creative Corp.
   Date of presentation: June 6, 2025

8.2 Cooperation and Sponsorship

This quarter, we cooperated with or sponsored the following events.

1. The 29th Shirahama Cyber Crime Symposium
   Organizer: Executive Committee of the Shirahama Cyber Crime Symposium
   Dates: May 22, 2025 – May 24, 2025
2. Interop Tokyo 2025
   Organizer: Interop Tokyo Executive Committee
   Dates: June 11, 2025 – June 13, 2025
3. Edge AI Initiative 2025
   Organizer: ITmedia Inc.
   Dates: June 17, 2025 – June 19, 2025

8.3 Public Materials

This section lists reports and blog posts on surveys and research published by JPCERT/CC this quarter.

8.3.1 Incident Handling Report

JPCERT/CC accepts reports on computer security incidents occurring in Japan and overseas, supports responses, understands the status of occurrence, analyzes methods, and provides advice to prevent recurrence. To present an overview of these activities, we publish, on a quarterly basis, statistical information such as the number of incident reports, the total number of reported incidents, and the number of coordinations conducted by JPCERT/CC in response to reports, as well as trends in incidents and incident response cases, in both Japanese and English reports. Note that publication via the Incident Handling Report ended in FY 2024. Please refer to this report, Chapter 1 Incident Response Support, going forward.

- 2025-04-17
  JPCERT/CC Incident Handling Report [January 1, 2025 – March 31, 2025] (Japanese)
  https://www.jpcert.or.jp/pr/2025/IR_Report2024Q4.pdf
- 2025-06-23
  JPCERT/CC Incident Handling Report [January 1, 2025 - March 31, 2025]
  https://www.jpcert.or.jp/english/doc/IR_Report2024Q4_en.pdf

8.3.2 Internet Threat Monitoring Report

JPCERT/CC has built and operates the Internet threat monitoring system TSUBAME, which distributes multiple sensors across the Internet to continuously collect packets sent to the general public. By classifying packets observed by the sensors and analyzing them against vulnerability information and information on malware and attack tools, we strive to capture attack activities and their preparatory activities. We compile the results of this Internet threat monitoring on a quarterly

basis and publish reports in Japanese and English.

- 2025-06-06
  JPCERT/CC Internet Threat Monitoring Report [January 1, 2025 – March 31, 2025] (Japanese)
  https://www.jpcert.or.jp/tsubame/report/report202501-03.html
  https://www.jpcert.or.jp/tsubame/report/TSUBAME_Report2024Q4.pdf
- 2025-06-23
  JPCERT/CC Internet Threat Monitoring Report [January 1, 2025 - March 31, 2025]
  https://www.jpcert.or.jp/english/doc/TSUBAMEReport2024Q4_en.pdf

8.3.3 Activity Report on Vulnerability-Related Information

IPA and JPCERT/CC, as the receiving organization and the coordination organization respectively, have been responsible since July 2004 for part of the operation of the vulnerability-related information handling scheme based on the Ministry of Economy, Trade and Industry Public Notice "Rules for Handling Vulnerability-Related Information on Software Products, etc." (METI Public Notice No. 19 of 2017, last amended METI Public Notice No. 93 of 2024), among others. We publish a report summarizing operational achievements for the previous quarter related to this scheme and notable trends in vulnerabilities disclosed during the same period.

- 2025-04-17
  Status of Reports on Vulnerability-Related Information for Software, etc. [Q1 2025 (January–March)]
  https://www.jpcert.or.jp/pr/2025/vulnREPORT_2025q1.pdf

8.3.4 Official Blog "JPCERT/CC Eyes"

The official blog of the JPCERT Coordination Center, "JPCERT/CC Eyes," quickly delivers content analyzed and investigated by JPCERT/CC, as well as coverage of domestic and international events and conferences, through the eyes of JPCERT/CC analysts.

This quarter, we published the following six articles.

Japanese edition: 3 articles https://blogs.jpcert.or.jp/ja/

- 2025-04-09
  Participation Report: RightsCon 2025
- 2025-04-24
  DslogdRAT Malware Installed in Ivanti Connect Secure
- 2025-06-06
  TSUBAME Report Overflow (January–March 2025)

English edition: 3 articles https://blogs.jpcert.or.jp/en/

- 2025-04-03
  JSAC2025 -Workshop & Lightning Talk-
- 2025-04-11
  ICS Security Conference 2025
- 2025-04-24
  DslogdRAT Malware Installed in Ivanti Connect Secure

Appendix A

Incident Categories

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 the JPCERT/CC website.

- JPCERT Coordination Center (JPCERT/CC): https://www.jpcert.or.jp/
- Providing incident information and requesting response: info@jpcert.or.jp, https://www.jpcert.or.jp/form/
- Inquiries regarding vulnerability information handling: vultures@jpcert.or.jp
- Inquiries regarding control system security: dc-info@jpcert.or.jp
- Inquiries regarding Secure Coding Seminar: secure-coding@jpcert.or.jp
- Citations of published materials, lecture requests, and other inquiries: pr@jpcert.or.jp
- About PGP public keys: https://www.jpcert.or.jp/jpcert-pgp.html

JPCERT/CC Quarterly Report [April 1, 2025 ～ June 30, 2025]

- Publication history
  - July 17, 2025 First Japanese version
  - October 24, 2025 First English version
- Issued by
  JPCERT Coordination Center
  8F Tozan Bldg, 4-4-2 Nihonbashi-Honcho, Chuo-ku, Tokyo 103-0023, Japan
  TEL 03-6271-8901 FAX 03-6271-8908
  URL https://www.jpcert.or.jp/