JPCERT/CC®

JPCERT/CC Quarterly Report

January 1, 2026 to March 31, 2026

April 16, 2026

JPCERT Coordination Center

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

The Japan Computer Emergency Response Team Coordination Center (hereinafter referred to as JPCERT/CC) conducts activities with the aim of contributing to the recognition and handling of computer security incidents (hereinafter referred to as incidents) within organizations that use the Internet, as well as to the prevention of the spread of damage caused by incidents. For incidents that require international coordination and support, we carry out coordination activities with relevant organizations in Japan and overseas as the point of contact in Japan.

We implement most of these activities as "Coordination Activities for International Cooperation in Responding to Cyber Attacks for the 2025 Fiscal Year" (a project commissioned by the Ministry of Economy, Trade and Industry) and "Verification Activities Concerning Methods to Facilitate the Collection of Technical Information on Attacks from Affected Organizations" (a project commissioned by the Cabinet Secretariat).

This document reports on activities from January 1, 2026 to March 31, 2026.

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" include some descriptions of voluntary activities other than sponsored activities.

Topics & Highlights

Holding JSAC2026

JSAC2026 was held at Tokyo from January 21 to January 23, 2026. This conference aims to share information about ever-changing attack techniques and new analysis methods in order to help improve the technical capabilities of security analysts who analyze and respond to security incidents caused by cyberattacks.

This ninth conference featured 20 presentations (including three workshops) selected from 91 submissions, as well as six presentations in the Lightning Talk session and a panel discussion. Technologies related to incident analysis, response, and countermeasures, such as incident response cases, analysis of threat actors, and recent trends in phishing attacks, were shared. In addition, this year, three analysis training sessions for analysts were conducted on the first day. On Training Day, 250 participants attended, and survey results showed that 98% of participants said they would like to

participate in the next training session as well. We plan to continue enhancing the training program next fiscal year.

On the second and third Conference Days, 405 participants attended, and lively discussions were held. Participants have praised JSAC as a valuable forum for sharing information among analysts, with numerous presentations that can only be heard at JSAC. The presentation materials are available on the JSAC2026 website. For an overview of the conference, please visit the JPCERT/CC Eyes blog.

- JSAC2026
  https://jsac.jpcert.or.jp/archive/2026/en/
- JSAC2026 -Day 1-
  https://blogs.jpcert.or.jp/en/2026/02/jsac2026day1.html
- JSAC2026 -Day 2-
  https://blogs.jpcert.or.jp/en/2026/02/jsac2026day2.html
- JSAC2026 -Workshop/Lightning Talk Session/Panel Discussion-
  https://blogs.jpcert.or.jp/en/2026/03/jsac2026-ws-lt-pd.html

Holding ICS Security Conference 2026

ICS Security Conference 2026 was held on February 10, 2026. This event began in 2009 with the aim of improving control system security in Japan. Due to the COVID-19 pandemic, it had been held online or in a hybrid format, but this year it returned to a fully in-person format, with 137 participants attending (216 preregistered). The program consisted of presentations selected through an open call and presentations planned by JPCERT/CC. Following opening remarks from the Ministry of Economy, Trade and Industry, a total of six presentations were given: two presentations by JPCERT/CC, one joint presentation by JPCERT/CC and external presenters, and three presentations by external presenters.

In the two presentations by JPCERT/CC, speakers reviewed the past year and explained various developments related to control system security, and also introduced international trends concerning vulnerability handling frameworks related to CVD. The joint presentation by JPCERT/CC and external presenters incorporated a panel discussion format, introduced initiatives by a community of security personnel from control system user organizations hosted by JPCERT/CC, and provided information useful for the work of control system users. In the three presentations by external presenters, speakers discussed the idea of applying “preparedness” developed in factories to cyber incident response, the background behind the growing use of digital twins in the automotive industry and defense methods against attacks targeting them. They also presented a method for organizing system structures using DFDs (Data Flow Diagrams) and integrating safety/security requirements, SBOMs, and decision-making histories into the same ledger (JSON). In addition, after the conference, an information exchange meeting was held, where speakers and participants alike deepened their connections through exchanging opinions and sharing information.

According to the survey results, the conference was attended by a wide range of participants, mainly control device/control system users, as well as control system engineering professionals, control system/control device vendors, and researchers. In addition, one in three survey respondents was a first-time participant, and we received valuable feedback from both returning and new participants.

The presentation materials are available on the JPCERT/CC website, and presentation videos are available on JPCERT/CC's YouTube channel. For an overview of the conference, please visit the JPCERT/CC Eyes blog.

- ICS Security Conference 2026
  https://www.jpcert.or.jp/event/ics-conference2026.html
- ICS Security Conference 2026 Presentation Materials
  https://www.jpcert.or.jp/present/#year2026
- ICS Security Conference 2026 Presentation Videos
  https://www.youtube.com/playlist?list=PLgEi6O-lWUIaE_ASwPJAjHVkOSYXjb3fY
- ICS Security Conference 2026 Event Report
  https://blogs.jpcert.or.jp/en/2026/04/ics-conference2026.html

Chapter 1

Incident Response Support

JPCERT/CC accepts reports of incidents that occur in Japan and overseas[*1]. In this chapter, we present incident reports accepted during this quarter from quantitative perspectives such as statistics and qualitative perspectives such as noteworthy cases.

1.1 Quarterly Statistical Information

The number of incident reports this quarter, the total number of reported incidents, and the number of cases coordinated by JPCERT/CC in response to the reports by month are shown in Table 1.1[*2].

The number of reports received this quarter was 15,345. Among these, the number of cases in which JPCERT/CC coordinated with relevant organizations in Japan and overseas was 3,168. Compared to the previous quarter, the number of reports decreased by 25% and the number of cases coordinated increased by 10%. Also, compared to the same period last year (number of reports: 10,102; number of cases coordinated: 3,974), the number of reports increased by 51% and the number of cases coordinated decreased by 20%.

The monthly trends over the past year for the number of reports and the number of cases coordinated

Table 1.1 Number of Incident Reports Related

	Jan	Feb	Mar	Total	Last Qtr.
Number of Reports	6,795	3,446	5,104	15,345	20,336
Number of Incidents	3,677	2,536	4,049	10,262	13,537
Cases Coordinated	943	991	1,234	3,168	2,875

[*1] JPCERT/CC refers to events that can be regarded as security issues in operating information systems, incidents related to computer security, and events in general as **incidents**.

[*2] **Number of reports** indicates the total number of reports submitted via the web form and by email by reporters. **Number of incidents** indicates the total number of incidents included in each report. Even if multiple reports are submitted regarding a single incident, it is counted as one. **Number of cases coordinated** indicates the number of cases in which we requested administrators of sites, etc. to investigate the current situation and take measures to resolve the issue to prevent the spread of the incident.

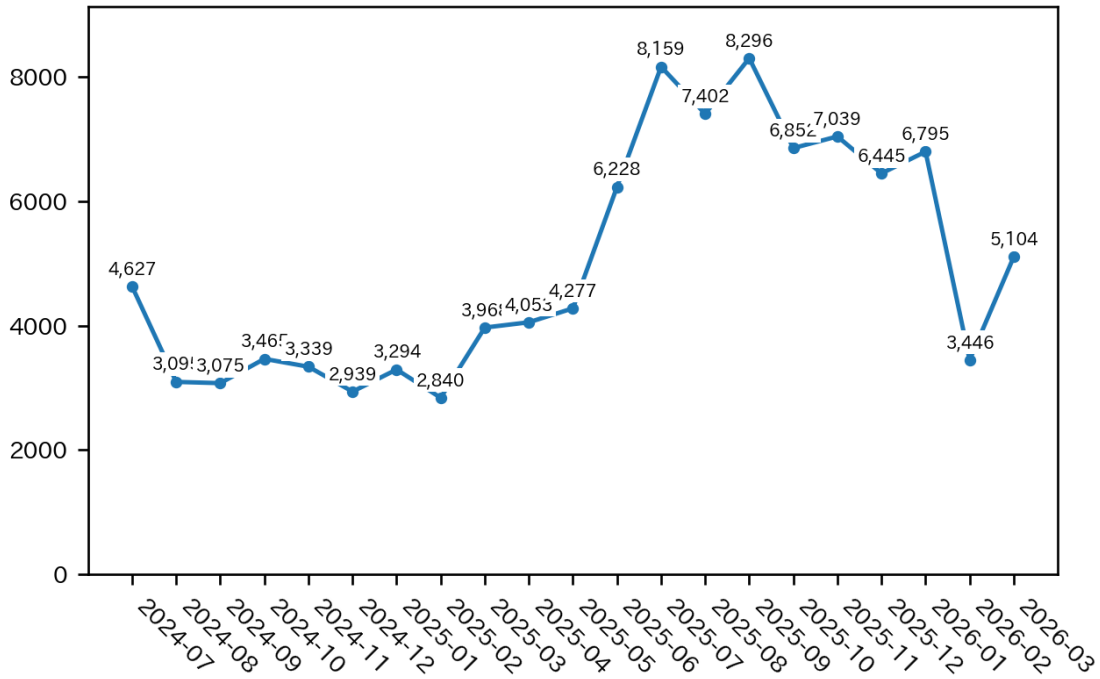

Figure 1.1 Trends in the Number of Incident Reports

Table 1.2 Number of Incident Reports by Category

Incident Category	Jan	Feb	Mar	Total	Last Qtr.
Phishing Site	3,421	2,227	3,645	9,293	12,397
Website Defacement	29	24	37	90	105
Malware Site	7	19	6	32	44
Scan	37	62	57	156	469
DoS/DDoS	0	1	3	4	6
ICS Related	0	0	0	0	0
Targeted Attack	0	0	2	2	3
Other	183	203	299	685	513

are shown in Figure 1.1 and Figure 1.2, respectively.

At JPCERT/CC, we classify reported incidents into categories and conduct coordination and responses according to the categories. For the definitions of each incident, please refer to **Appendix A Incident Categories**. The breakdown by category of the number of incident reports received this quarter is shown in Table 1.2 and the percentages by category are shown in Figure 1.3.

Incidents classified as phishing sites accounted for 90.6%, and incidents classified as scans, which probe system vulnerabilities, accounted for 1.5%.

The monthly trends over the past year for each of the following incidents—phishing sites, website defacement, malware sites, and scans—are shown in Figure 1.4 through Figure 1.7.

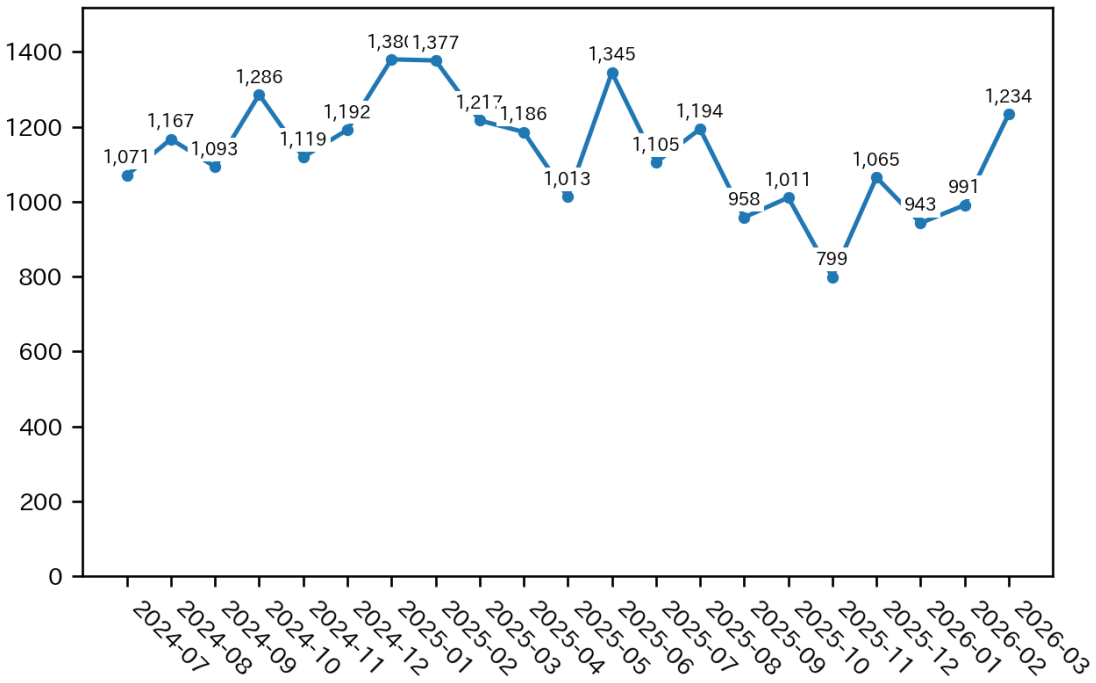

Figure 1.2 Trends in the Number of Cases Coordinated

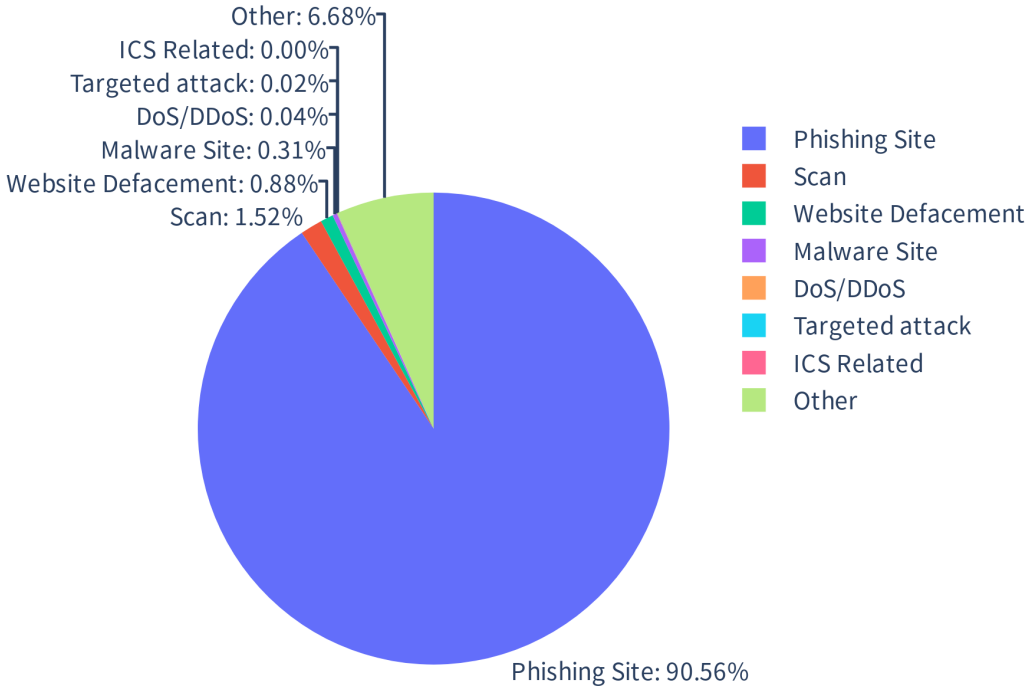

Figure 1.3 Percentage of the Number of Incident Reports by Category

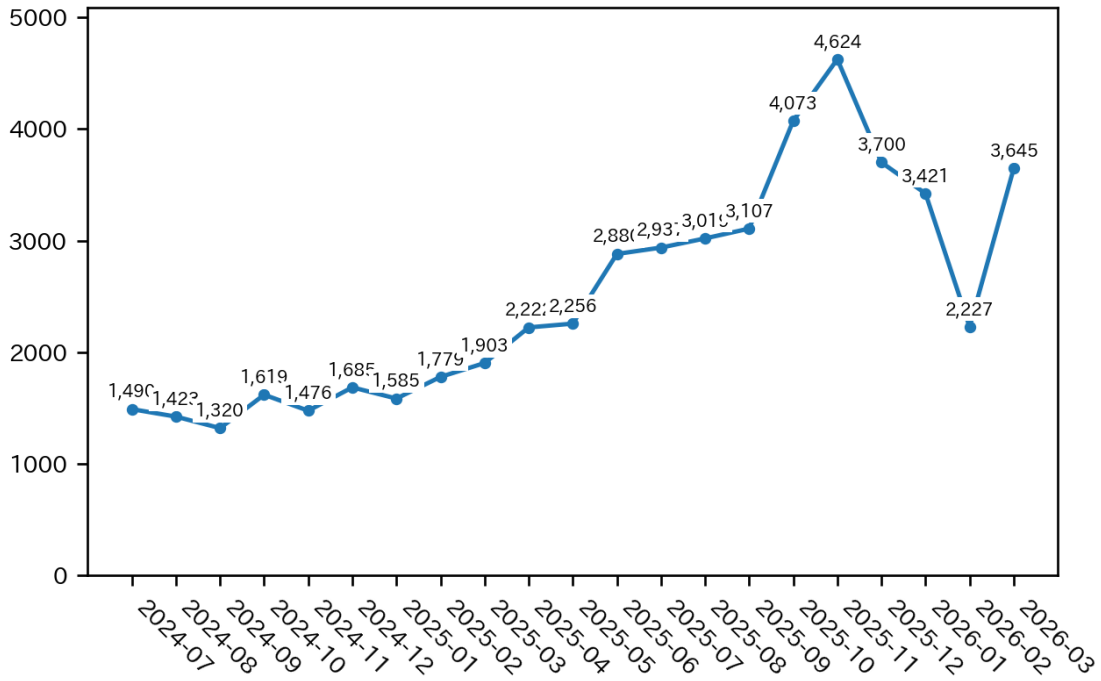

Figure 1.4 Trends in the Number of Phishing Sites

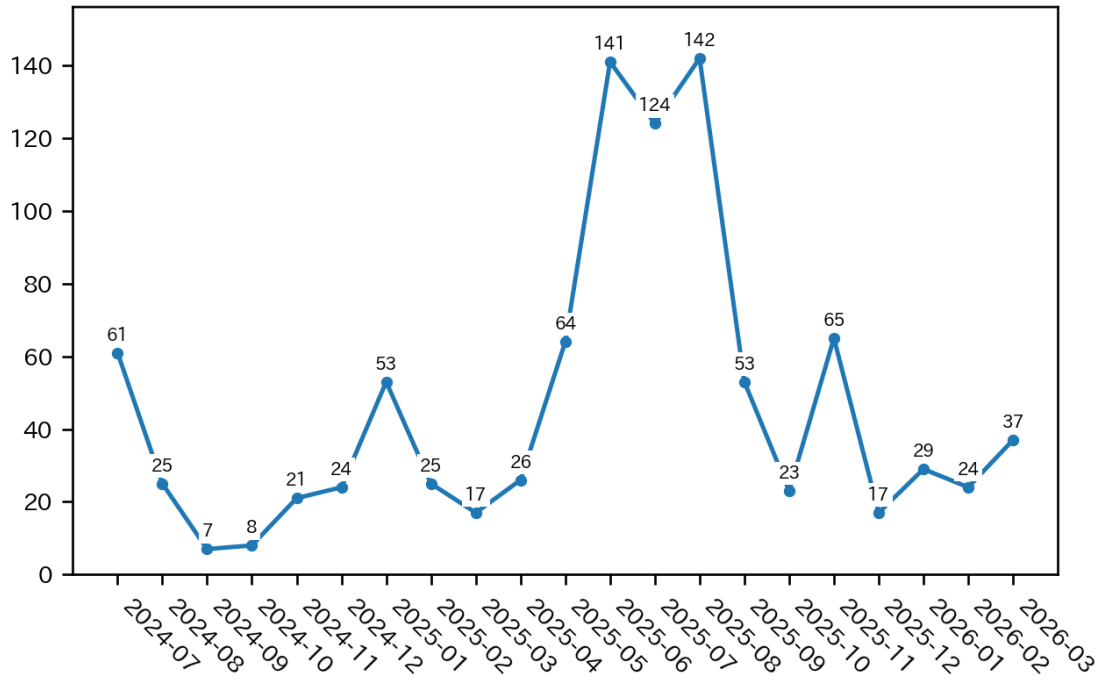

Figure 1.5 Trends in the Number of Website Defacements

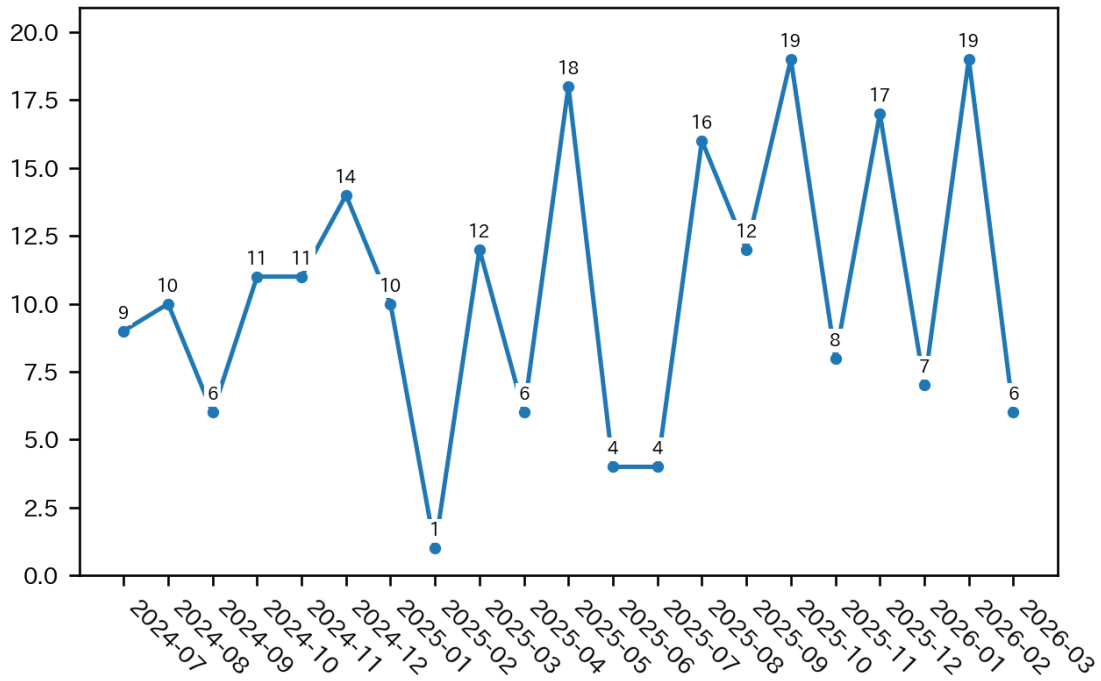

Figure 1.6 Trends in the Number of Malware Sites

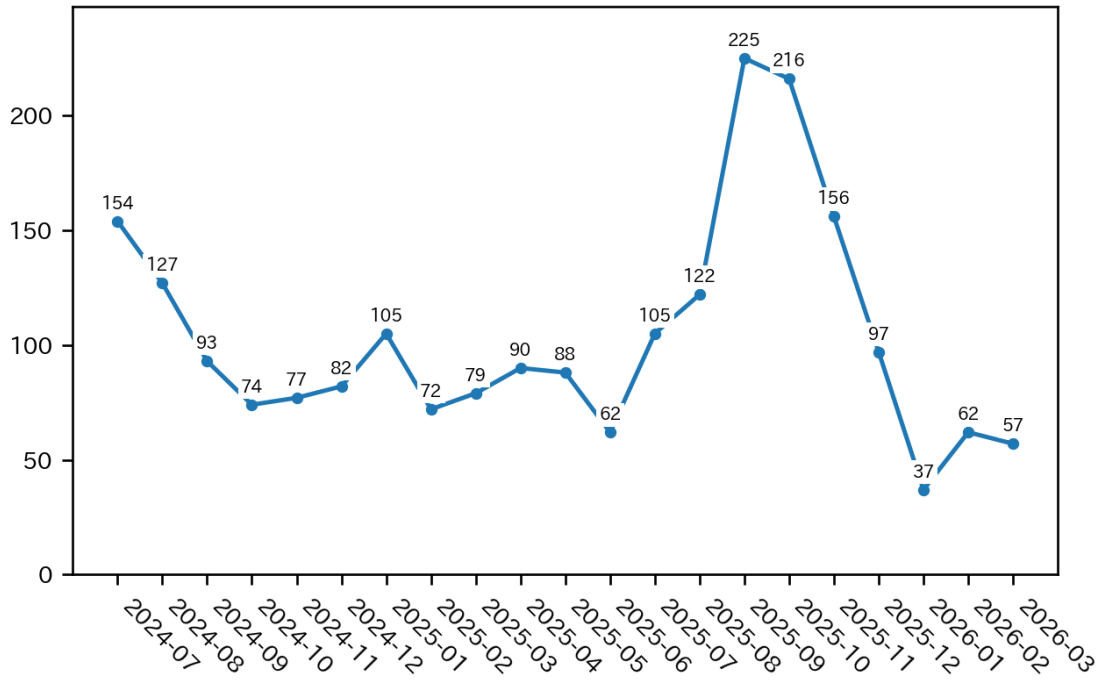

Figure 1.7 Trends in the Number of Scans

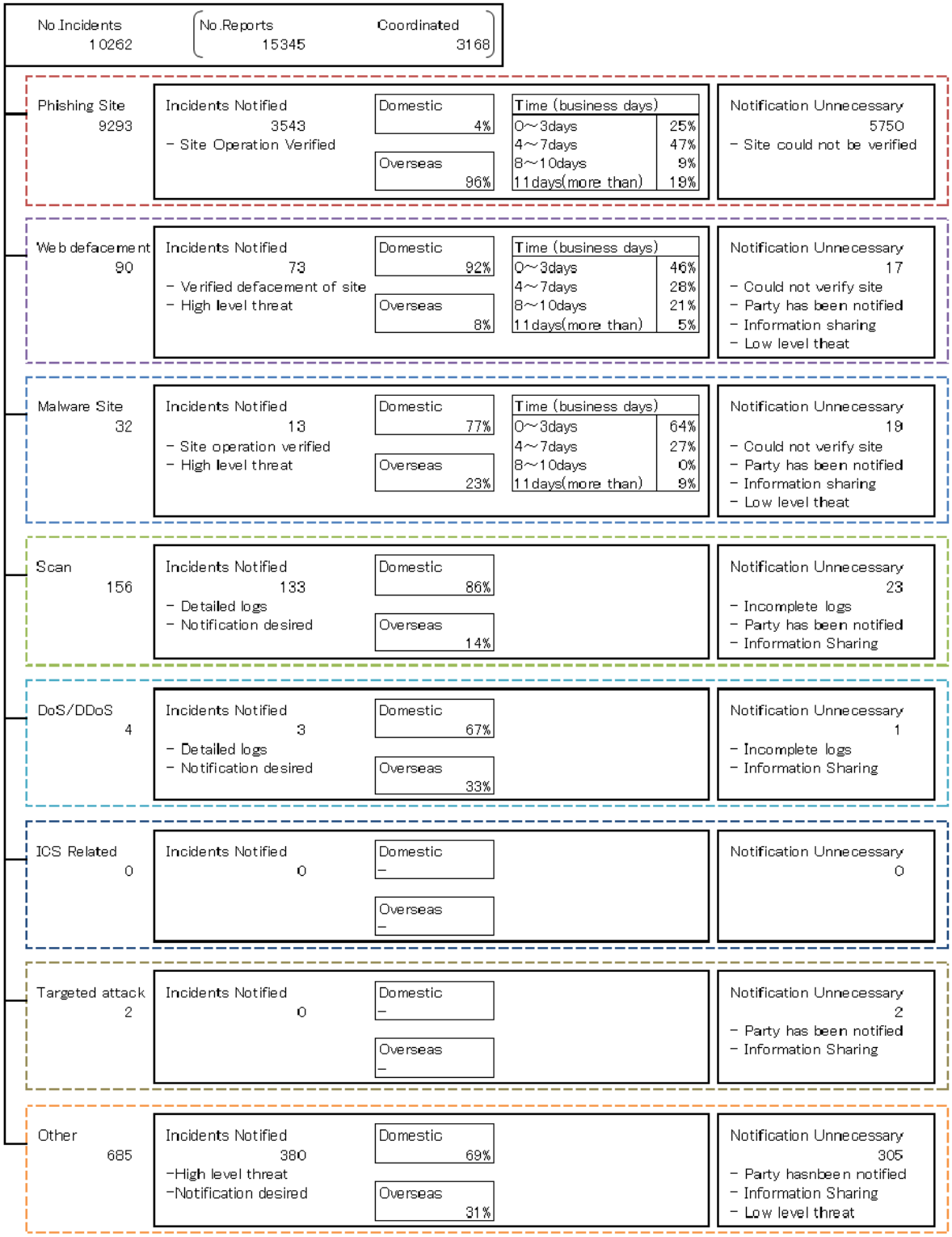

Figure 1.8 Number of Cases and Coordination/Response Status by Incident Category

The number of cases and the coordination/response status for each incident category are also shown in Figure 1.8.

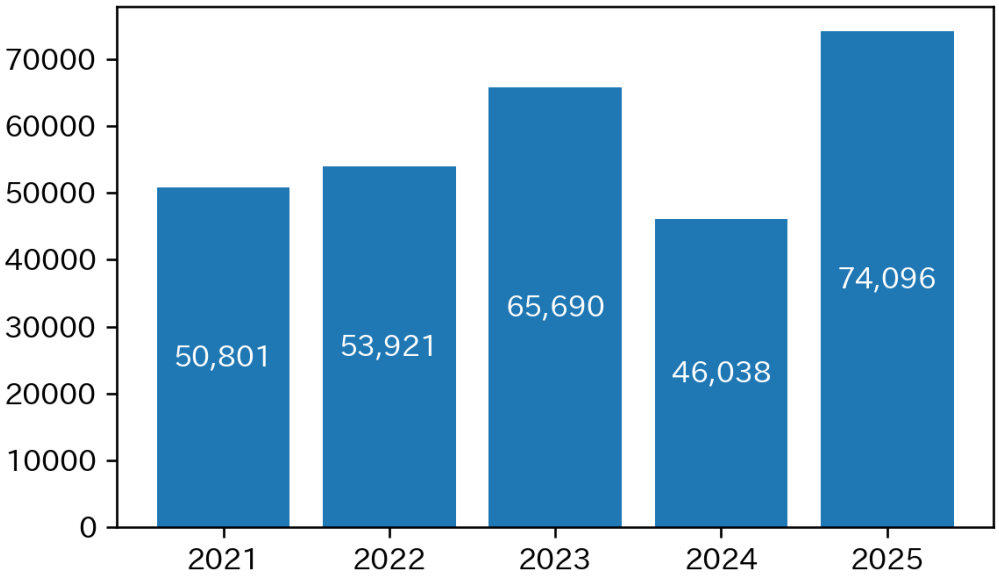

Figure 1.9 Annual Trend in the Number of Incident Reports

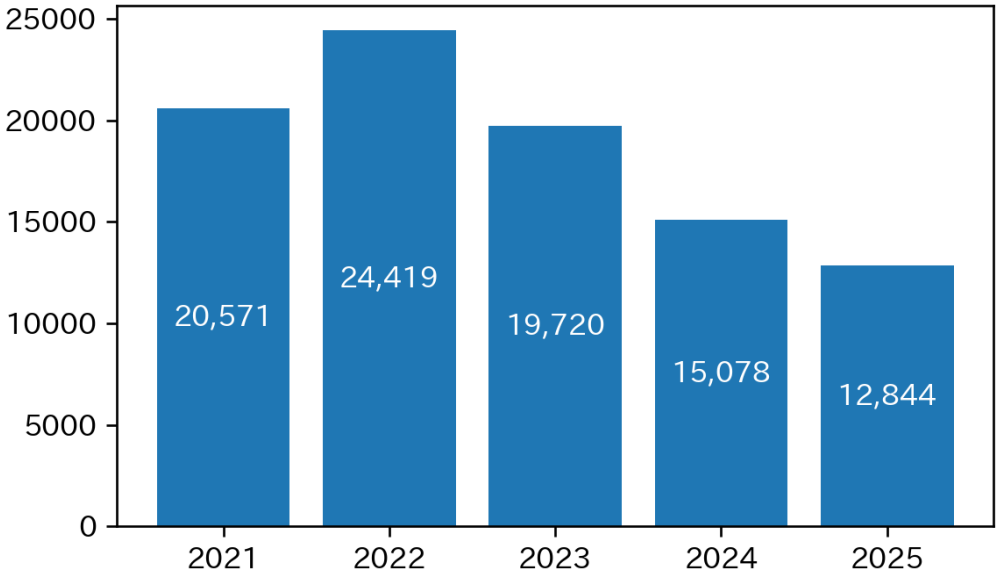

Figure 1.10 Annual Trend in the Number of Cases Coordinated

1.2 Annual Statistical Information

The annual trend in the number of incident reports for the past 5 years up to this fiscal year is shown in Figure 1.9, and the trend in the number of cases coordinated is shown in Figure 1.10. The number of reports received this fiscal year was 74,096. This was a 61% increase compared to 46,038 in the previous fiscal year. The number of cases coordinated this fiscal year was 12,844. This was a 15% decrease compared to 15,078 in the previous fiscal year.

Table 1.3 Number of Phishing Sites for Domestic and Overseas Brands

Phishing Site	Jan	Feb	Mar	Total	Pct.
Domestic Brand	2,644	1,448	3,020	7,112	76%
Overseas Brand	199	377	323	899	10%
Unknown Brand	578	402	302	1,282	14%
Monthly Total	3,421	2,227	3,645	9,293	

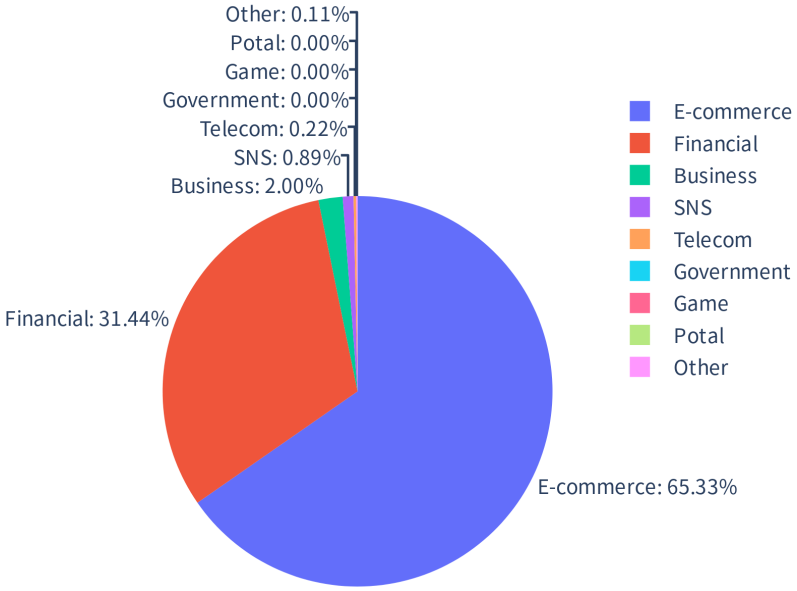

Figure 1.11 Percentage of the Number of Phishing Sites for Overseas Brands by Industry

1.3 Incident Trends

1.3.1 Trends in Phishing Sites

The number of phishing sites reported this quarter was 9,293, a 25% decrease from the previous quarter's 12,397. This was also a 76% increase compared to the same period last year (5,267).

This quarter, the number of phishing sites impersonating overseas brands was 899, a 58% increase from the previous quarter's 569. The number of phishing sites impersonating domestic brands was 7,112, a 32% decrease from the previous quarter's 10,532. The breakdown of phishing site counts this quarter by domestic/overseas brand [*3] is shown in Table 1.3, and the percentages for phishing sites impersonating overseas and domestic brands by industry are shown in Figure 1.11 and Figure 1.12, respectively.

Among the phishing sites reported to JPCERT/CC, 65.3% of the reports related to overseas brands impersonated e-commerce sites, and 69.1% of the reports related to domestic brands impersonated

[*3] **Unknown Brand** indicates the number of sites for which the brand could not be identified because the reported phishing site had been taken down at the time of confirmation, among other reasons.

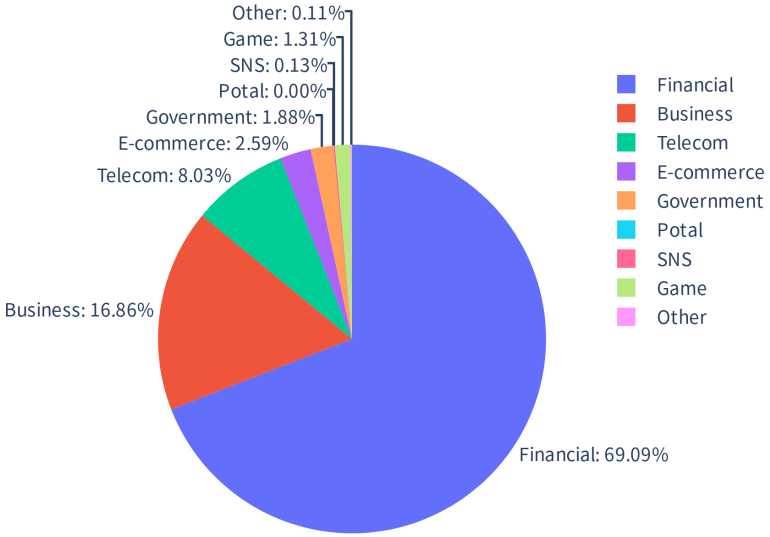

Figure 1.12 Percentage of the Number of Phishing Sites for Domestic Brands by Industry

financial sites, the largest shares in each.

For overseas brands, many phishing sites impersonated Amazon and Apple Account. For domestic brands, many reports concerned phishing sites impersonating securities companies such as Monex, Inc., SBI Securities, and SMBC Nikko Securities Inc. Also, many were still reported for credit card companies such as JCB, Sumitomo Mitsui Card, and Saison Card. Of the sites for which we coordinated takedown of phishing sites, 96% were overseas and 4% were domestic.

1.3.2 Trends in Website Defacement

The number of website defacements reported this quarter was 90. This was a 14% decrease from the previous quarter's 105.

This quarter, JPCERT/CC confirmed the following website defacement cases.

- Case 1: A web shell was installed on a legitimate website
- Case 2: A legitimate website was defaced as part of possible "Efimer" malware propagation activity

In Case 1, the same web shell (Figure 1.13) had been installed on multiple legitimate websites in Japan. Using the installed web shell, the attacker may have executed arbitrary commands or defaced content.

In Case 2, multiple websites built with WordPress in Japan had been defaced, and files containing the string "0x1c8c5b6a" had been placed on them. It has been pointed out that websites containing this string may have been used by attackers to make unauthorized posts or write entries, and that they were defaced as part of propagation activity for the malware "Efimer."

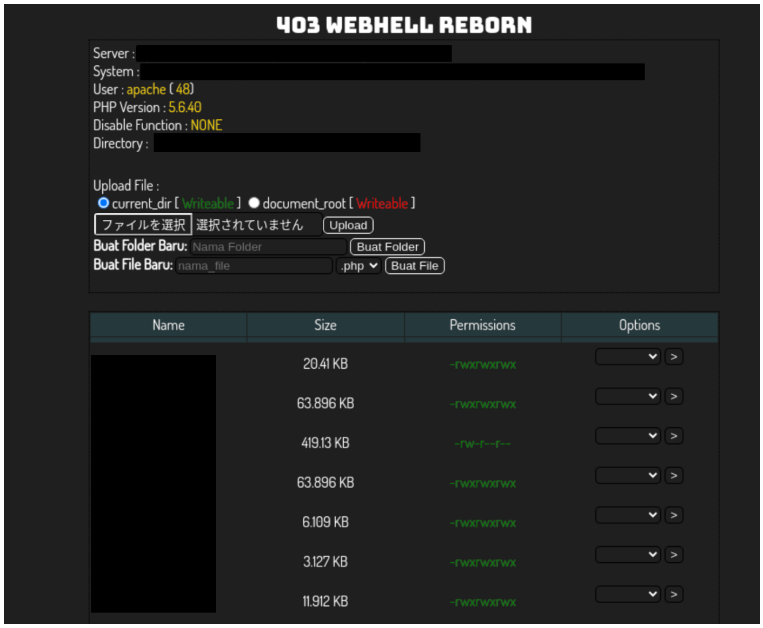

Figure 1.13 Web Shell

- Security Alert Regarding WordPress Site Defacement and the Trojan “Efimer”
  https://www.lac.co.jp/lacwatch/alert/20250826_004473.html

1.3.3 Trends in Targeted Attacks

The number of incidents classified as targeted attacks was 2.

1.3.3.1 Targeted Attack Emails Abusing GitHub

This quarter, JPCERT/CC received reports of targeted attack emails abusing GitHub. Clicking a link in the email body downloaded a ZIP file, and executing an LNK file in the ZIP file caused a decoy document and PowerShell file stored on GitHub to be executed. The PowerShell file uploaded device information to GitHub as a text file, and if the uploaded information indicated that the device was a target, further attack activity was likely to be carried out. Note that this attack has similarities to an attack campaign reported by Trellix in August 2025 and may be part of the same type of attack campaign.

- The Coordinated Embassy Hunt: Unmasking the DPRK-linked GitHub C2 Espionage Campaign
  https://www.trellix.com/blogs/research/dprk-linked-github-c2-espionage-campaign/

1.3.4 Trends in Other Incidents

The number of malware sites reported this quarter was 32. This was a 27% decrease from 44 in the previous quarter.

Table 1.4 Top 10 Ports by Number of Scans

Port	Jan	Feb	Mar	Total
23/tcp	25	26	7	58
80/tcp	2	4	14	20
443/tcp	1	7	4	12
81/tcp	1	2	2	5
8000/tcp	0	2	3	5
8080/tcp	0	1	4	5
5555/tcp	2	2	0	4
82/tcp	0	1	3	4
9000/tcp	0	0	4	4
85/tcp	0	3	0	3

The number of scans reported this quarter was 156. This was a 66% decrease from 469 in the previous quarter. The top 10 most targeted ports for scans are shown in Table 1.4. Ports frequently targeted by scans were Telnet (23/TCP), HTTP (80/TCP), HTTPS (443/TCP), and 81/TCP.

The number of incidents classified as Other was 685. This was a 34% increase from 513 in the previous quarter.

1.4 Incident Response Cases

This section introduces cases handled this quarter.

1.4.1 Phishing Cases Using Compromised Overseas Websites as Stepping Stones

We received many reports of legitimate websites that had been defaced by attackers, turned into SEO spam, and abused to redirect users to phishing sites. As a result of investigating the many reported domains, we confirmed that many of the targets were operated in hosting environments outside Japan. For this reason, we shared relevant information with National CSIRTs in each country and coordinated so that security alerts and responses would be carried out for site administrators and hosting providers.

1.4.2 Response to Support Scam Cases Displaying Fake Warning Screens

We received many reports of cases in which fake security warning screens were displayed while users were browsing legitimate websites, prompting them to contact a support desk. Although these reports were submitted as phishing, investigation confirmed behavior highly likely to be what is known as a support scam, such as the display of fake warning screens. JPCERT/CC coordinated

with the administrators of legitimate websites where security warning screens were displayed.

Chapter 2

Analysis and Provision of Threat Intelligence

To prevent the occurrence and spread of damage caused by incidents, JPCERT/CC collects and analyzes vulnerability information, threat intelligence, and security information. When our analysis determines that the likelihood of the occurrence and spread of damage caused by incidents has increased, we provide alert information such as "Security Alerts" and "Early Warning Information", as well as information for handling and countermeasures against incidents.

2.1 Information Collection and Analysis

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

We also collect feedback from organizations regarding the information JPCERT/CC provides, which helps us understand the impact in Japan and conduct further analysis. In particular, feedback from organizations via the portal site "CISTA (Collective Intelligence Station for Trusted Advocates)" (see 2.3) that provides Early Warning Information, among others, is effectively utilized, including sharing it with other organizations.

This section highlights notable items among the information collected, feedback received, and analyses conducted this quarter.

2.1.1 Vulnerability in React Server Components (CVE-2025-55182)

On December 3, 2025 (local time), The React Team published an advisory [*1] regarding a vulnerability in React Server Components (CVE-2025-55182). React Server Components is a mechanism that performs part of React rendering on the server side and sends the results to the client. This

[*1] "Critical Security Vulnerability in React Server Components." The React Team. https://react.dev/blog/2025/12/03/critical-security-vulnerability-in-react-server-components, (2025-12-03)

vulnerability may allow an attacker to execute arbitrary code without authentication by sending a crafted HTTP request (a malicious Flight payload via HTTP) to a server that uses React Server Components (RSC). Although JPCERT/CC had not confirmed information such as observations of exploitation of this vulnerability, it published a CyberNewsFlash [*2] on December 5, 2025, to broadly call for early implementation of countermeasures. This was because the vulnerability allows arbitrary code execution without authentication, and major frameworks that use React Server Components, such as Next.js, are widely adopted in Japan and were expected to affect a wide range of systems.

After that, JPCERT/CC received multiple reports concerning exploitation of this vulnerability. These included cases suggesting that the vulnerability was exploited in a relatively short period after its disclosure and that multiple attackers may have conducted attacks over a wide area. As in this case, attacks that cause serious impact on systems through remote arbitrary code execution are increasingly occurring over a wide area shortly after vulnerabilities are disclosed, making prompt application of patches more important. In light of the actual attack activities confirmed, JPCERT/CC published a blog article [*3] summarizing the attack timeline and analysis of the malware used.

There was also a case in which this vulnerability was exploited to deface websites and display a message urging response to the vulnerability. When accessing the defaced websites, a warning was displayed in four languages stating that patches needed to be applied immediately because of the CVE-2025-55182 vulnerability. As a result of investigation, it was found that about 50 websites had been defaced, and individual notifications were sent to the administrators of the affected sites and others.

2.1.2 Information Disclosure Vulnerability in MongoDB (CVE-2025-14847)

On December 19, 2025 (local time), MongoDB published an advisory [*4] regarding an information disclosure vulnerability in MongoDB from uninitialized heap memory (CVE-2025-14847). This vulnerability allowed an unauthenticated remote third party to read information remaining in uninitialized heap memory by sending crafted communications, which could ultimately lead to the disclosure of confidential information in MongoDB (such as API keys and credentials).

Multiple security companies published blog articles [*5] that included explanations of proof-of-concept code for this vulnerability, and JPCERT/CC also confirmed information [*6] suggesting exploitation

[*2] "Vulnerability in React Server Components (CVE-2025-55182)." JPCERT/CC. https://www.jpcert.or.jp/newsflash/2025120501.html, (2025-12-05)

[*3] "Multiple Threat Actors Rapidly Exploit React2Shell: A Case Study of Active Compromise." JPCERT/CC. https://blogs.jpcert.or.jp/ja/2026/02/react2shell.html, (2026-02-13)

[*4] "Make minimally sized buffers for uncompressed Messages." MongoDB. https://jira.mongodb.org/browse/SERVER-115508, (2025-12-19)

[*5] "MongoBleed (CVE-2025-14847): MongoDB Memory Leak Flaw." Rapid7. https://www.rapid7.com/blog/post/etr-mongobleed-cve-2025-1484-critical-memory-leak-in-mongodb-allowing-attackers-to-extract-sensitive-data/, (2025-12-29)

[*6] "MongoBleed CVE-2025-14847: Critical Memory Leak in MongoDB Allowing Attackers to Extract Sensitive Data." Resecurity. https://www.resecurity.com/blog/article/mongobleed-cve-2025-14847-mongodb-memory-leak-flaw, (2025-12-30)

of this vulnerability overseas. There have been multiple past vulnerabilities similar to this one in which information in memory could be read. Among them, CitrixBleed (CVE-2023-4966) had a major social impact, including a case [*7] in which the ransomware group LockBit was confirmed to have exploited it for initial intrusion. Against this background, JPCERT/CC was concerned that attacks exploiting this vulnerability might spread to Japan and published a CyberNewsFlash [*8] on January 6, 2026.

The Shadowserver Foundation shared information with JPCERT/CC on about 120 domestic hosts that may be affected by this vulnerability. This number of hosts increased further, reaching about 600 as of mid-January 2026. In response, JPCERT/CC sent individual notifications to hosting providers, which accounted for the majority of the hosts, asking them to inform their contracted users about the response. JPCERT/CC also individually notified companies that had not made progress in responding to this vulnerability and urged them to take action.

2.1.3 Vulnerabilities in Cisco Secure Email Gateway and Cisco Secure Email and Web Manager (CVE-2025-20393)

On December 17, 2025 (local time), Cisco published an advisory [*9] regarding attack activity targeting vulnerabilities in Cisco Secure Email Gateway and Cisco Secure Email and Web Manager. This vulnerability (CVE-2025-20393, CVSS base score: 10.0) allows arbitrary command execution with root privileges when the "Spam Quarantine" feature is enabled and operated while exposed to the Internet. It has been reported that exploitation had occurred by late November 2025 at the latest, before the vulnerability was publicly disclosed.

JPCERT/CC had received reports of compromise of the products before this vulnerability was published, and because it also confirmed that about 10 hosts in Japan were operating in a state in which the vulnerability could be exploited, it individually notified user organizations immediately after the publication. In addition, while continuing to observe the distribution status of vulnerability information and the progress of responses in collaboration with the developer and sales agents, JPCERT/CC found that knowledge regarding investigations when lateral movement occurred after compromise had not been sufficiently disseminated to related organizations. Therefore, with permission from the parties concerned, JPCERT/CC shared the investigation findings obtained through individual notifications and information on the attacks, enabling them to be used for investigations at other organizations.

[*7] "CVE-2023-4966: LockBit Exploits Citrix Bleed in Ransomware Attacks." Picus Security. https://www.picussecurity.com/resource/blog/cve-2023-4966-lockbit-exploits-citrix-bleed-in-ransomware-attacks, (2024-05-09)

[*8] "Information Disclosure Vulnerability in MongoDB (CVE-2025-14847)." JPCERT/CC. https://www.jpcert.or.jp/newsflash/2026010601.html, (2026-01-06)

[*9] "Reports About Cyberattacks Against Cisco Secure Email Gateway And Cisco Secure Email and Web Manager." Cisco. https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sma-attack-N9bf4, (2025-12-17)

2.1.4 Listing on the Leak Site of the 0apt Ransomware Group

From late January to early February 2026, the ransomware group "0apt" posted approximately 200 claims of compromise at once, including claims involving Japanese companies, on a leak site believed to be managed by the group. Based on JPCERT/CC's analysis of posted organization names and other information, nonexistent organization names were mixed in, and data samples or technical evidence supporting the compromises were lacking. JPCERT/CC therefore assessed that the credibility of the claims of compromise in this case was low. Around the same time, a sample of ransomware believed to be used by the group was identified. In addition to AES-256 and RSA, the sample used the "Speck" cipher, and it was also pointed out [*10] that part of the code had characteristics that appeared to be AI-generated. JPCERT/CC individually notified four of the listed organizations that it was able to contact and exchanged information on each organization's response policies and other matters while conveying JPCERT/CC's view of the situation.

2.1.5 Vulnerabilities in Ivanti Endpoint Manager Mobile (EPMM) (CVE-2026-1281, CVE-2026-1340)

On January 29, 2026 (local time), Ivanti published an advisory regarding remote code execution vulnerabilities in Ivanti Endpoint Manager Mobile (EPMM) (CVE-2026-1281, CVE-2026-1340). If these vulnerabilities are exploited, an unauthenticated attacker may be able to execute arbitrary code. At the time of publication, Ivanti stated that it had confirmed exploitation of these vulnerabilities in a very small number of customer environments. JPCERT/CC confirmed the use in Japan of products that may be affected by these vulnerabilities and, in anticipation of a proof of concept for the vulnerabilities being made public in the future, published a Security Alert [*11] on January 30, 2026, the following day, with the aim of deterring activity by opportunistic attackers.

In addition, because the products were confirmed to be running on about 40 hosts in Japan, JPCERT/CC individually notified some user organizations and recommended early application of countermeasures and implementation of investigations. On January 30, 2026 (local time), an article explaining a proof of concept for the vulnerabilities was published [*12], and attacks exploiting these vulnerabilities were subsequently confirmed to have spread. JPCERT/CC comprehensively analyzed information obtained from partner organizations in Japan and overseas and from notification recipients, as well as publicly available information, and provided target organizations with information on traces of attacks useful for investigation.

[*10] "0APT Ransomware – The Real Fake?". The Raven File. https://theravenfile.com/2026/02/14/0apt-ransomware-the-real-fake/, (2026-02-14)

[*11] "Security Alert Regarding Vulnerabilities in Ivanti Endpoint Manager Mobile (EPMM) (CVE-2026-1281, CVE-2026-1340)." JPCERT/CC. https://www.jpcert.or.jp/at/2026/at260002.html, (2026-01-30)

[*12] "Someone Knows Bash Far Too Well, And We Love It (Ivanti EPMM Pre-Auth RCEs CVE-2026-1281 & CVE-2026-1340)." watchTowr. https://labs.watchtowr.com/someone-knows-bash-far-too-well-and-we-love-it-ivanti-epmm-pre-auth-rces-cve-2026-1281-cve-2026-1340/, (2026-01-30)

2.1.6 OS Command Injection Vulnerability in FileZen (CVE-2026-25108)

On February 13, 2026, Soliton Systems K.K. published information [*13] regarding an OS command injection vulnerability in FileZen (CVE-2026-25108). A user logged on to the product may exploit this vulnerability to execute arbitrary OS commands, and Soliton Systems stated that it had confirmed exploitation of this vulnerability at the time of publication. The company had reported this vulnerability to JPCERT/CC before publication, and in response, JPCERT/CC proceeded with coordination and published vulnerability information (JVN#84622767: OS Command Injection Vulnerability in FileZen) [*14] on JVN on the same day as the company's publication. For details, please see Section 4.1.2.1.

The company released countermeasures for this vulnerability on January 13, 2026, but JPCERT/CC had confirmed at that time that a considerable number of products potentially affected by this vulnerability were in use in Japan. Therefore, on February 13, 2026, JPCERT/CC published a Security Alert [*15] and broadly called for implementation of countermeasures against this vulnerability. In addition, because the product was also used by government ministries and agencies, local governments, and other organizations, JPCERT/CC individually notified and provided information to relevant organizations.

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 distributed by email to subscribers of the mailing list (about 42,000 as of the end of this quarter).

2.2.1 Security Alerts

When critical vulnerabilities with a wide impact are disclosed, we publish a Security Alert to broadly call on users to take countermeasures.

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

This quarter, we published 8 items.

- 2026-01-14

[*13] "Important: Command Injection Vulnerability on FileZen Post-logon Screen." Soliton Systems K.K. https://www.soliton.co.jp/support/2026/006657.html, (2026-02-13)

[*14] "JVN#84622767 OS Command Injection Vulnerability in FileZen." JVN. https://jvn.jp/jp/JVN84622767/, (2026-02-13)

[*15] "Security Alert Regarding OS Command Injection Vulnerability in FileZen (CVE-2026-25108)." JPCERT/CC. https://www.jpcert.or.jp/at/2026/at260004.html, (2026-02-13)

Security Alert Regarding the January 2026 Microsoft Security Updates (Publication)

- 2026-01-30

Security Alert Regarding Vulnerabilities in Ivanti Endpoint Manager Mobile (EPMM) (CVE-2026-1281, CVE-2026-1340) (Publication)

- 2026-02-12

Security Alert Regarding the February 2026 Microsoft Security Updates (Publication)

- 2026-02-13

Security Alert Regarding an OS Command Injection Vulnerability in FileZen (CVE-2026-25108) (Publication)

- 2026-03-11
  Security Alert Regarding the March 2026 Microsoft Security Updates (Publication)
- 2026-03-11
  Security Alert Regarding Vulnerabilities in Adobe Acrobat and Reader (APSB26-26) (Publication)
- 2026-03-30
  Security Alert Regarding a Vulnerability in F5 BIG-IP Access Policy Manager (CVE-2025-53521) (Publication)
- 2026-03-31
  Security Alert Regarding an Out-of-bounds Read Vulnerability in NetScaler ADC and NetScaler Gateway (CVE-2026-3055) (Publication)

2.2.2 CyberNewsFlash

JPCERT/CC may publish information that does not meet the criteria for a Security Alert at the time of publication—such as information about vulnerabilities, malware, and cyberattacks—as "CyberNewsFlash."

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

This quarter, we published 1 item and updated 1 item.

- 2026-01-06
  Information Disclosure Vulnerability in MongoDB (CVE-2025-14847)
- 2026-01-07

Vulnerability in React Server Components (CVE-2025-55182) (Update)

2.2.3 Weekly Report

Among the security-related information collected by JPCERT/CC, we compile summaries of information deemed important and, in principle, publish them every Wednesday (the third business day of each week) as the "Weekly Report." This quarter, we published 12 issues and provided a total of 120 security information items.

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

2.3 Information Provided via CISTA

JPCERT/CC operates CISTA, a registration-based information-sharing platform. We accept registrations from those who wish to receive Early Warning Information and share information with about 1,300 organizations, including information security departments that support critical infrastructure and internal CSIRTs.

For details about the Early Warning Information framework, please refer to the following web page.

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

On CISTA, recipient organizations can provide feedback and reply to the information provided by JPCERT/CC. We leverage and give back the feedback and replies we receive by providing information to other organizations, within permitted sharing scopes, among other uses.

2.3.1 Early Warning Information

Among the collected information on vulnerabilities and threats, those assessed as potentially having a significant impact on critical information infrastructure and requiring early dissemination to organizations that provide such infrastructure are shared as Early Warning Information. This quarter, 4 items were sent.

2.3.2 Analyst Note

Among the collected vulnerability information and threat intelligence, items that JPCERT/CC considers noteworthy are compiled daily and provided as Analyst Note. This quarter, 58 Analyst Notes were sent.

2.3.3 Individually Provided Information

From the collected information, we provide vulnerability information and threat intelligence individually for items that are considered to affect specific organizations. For example, we provide information to organizations that use hosts in a "vulnerable host" state, such as not having applied countermeasures for serious vulnerabilities, or hosts that may already have had unauthorized programs installed, been defaced, or had credentials stolen due to exploitation of vulnerabilities. If we cannot provide information individually to the target organization via CISTA, we may notify the contact registered in JPNIC WHOIS, or ask the ISP or maintenance vendor to notify them. This quarter, JPCERT/CC provided 30 items. We provided information to organizations that manage hosts affected by the vulnerability information and threat intelligence mentioned above, among others.

Chapter 3

Observation and Analysis of Reconnaissance and Attack Activities on the Internet

JPCERT/CC has developed monitoring sensors that collect packets sent to a large number of unspecified hosts and has built and continues to operate the Internet Threat Monitoring System "TSUBAME" by distributing multiple sensors domestically and overseas using hosting services, among others. Packets received by the sensors are considered to be attempts to discover specific devices or service functions. JPCERT/CC continuously collects packets observed by sensors and analyzes them in comparison with vulnerability information and information on malware and attack tools. The analysis can reveal attack activities over the Internet and preparatory activities for attacks, enabling rapid identification of global attack activities.

3.1 Monitoring Using the Internet Threat Monitoring System "TSUBAME"

TSUBAME records TCP, UDP, and ICMP packets among the packets that reach the sensors from the Internet. Note that unlike honeypots, the sensors do not respond to packets that reach them. TSUBAME monitors traffic that poses security threats, such as worm infection activities and scans to probe for vulnerabilities.

For more information about TSUBAME, please refer to the following web page.

- TSUBAME (Internet Threat Monitoring System)
  https://www.jpcert.or.jp/tsubame/index.html

3.1.1 Utilization of TSUBAME Observation Data

JPCERT/CC provides observation data obtained from TSUBAME so that system administrators in organizations can use it for incident response and countermeasures. In addition to providing individualized information based on observation data on a quarterly basis, we publish the Internet

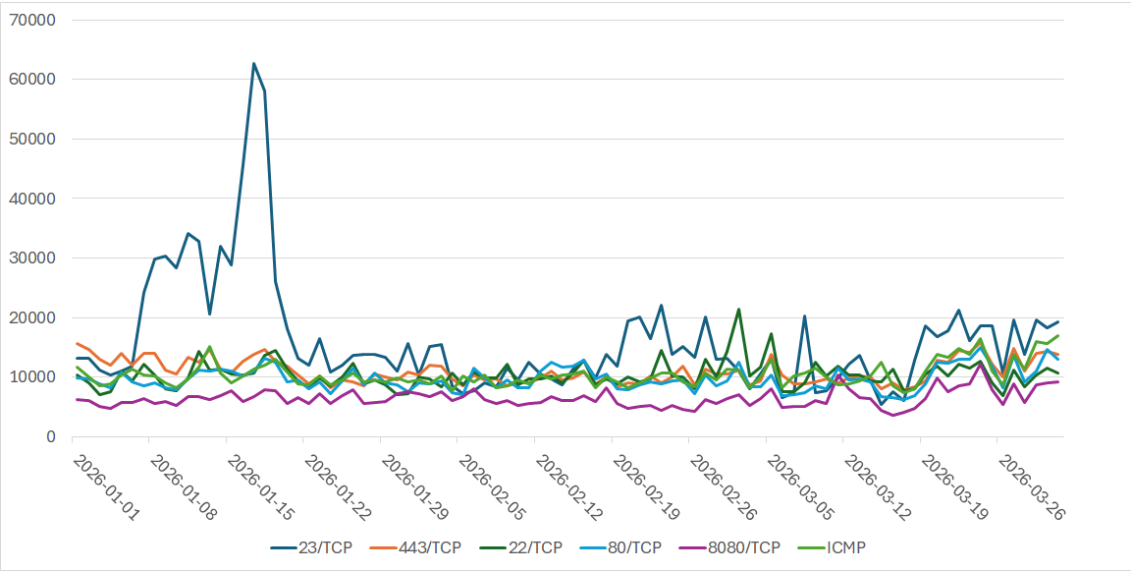

Figure 3.1 Packet Counts for Top-Ranked Destination Ports 1–5 Observed by TSUBAME (January 1, 2026–March 31, 2026)

Threat Monitoring Report and the blog "TSUBAME Report Overflow," which introduce observation trends and noteworthy phenomena. The blog covers analysis that could not be fully included in the report and notable events that occurred during the period.

- JPCERT/CC Internet Threat Monitoring Report
  https://www.jpcert.or.jp/tsubame/report/
- TSUBAME Report Overflow
  https://blogs.jpcert.or.jp/ja/tags/tsubame/

3.1.2 TSUBAME Observation Trends

The figure shows an aggregation by destination port of the packets received by TSUBAME sensors in Japan this quarter[*1]. Please refer to this when analyzing trends in packets reaching an organization's network.

For the destination ports that ranked in the top 10 by total number of packets this quarter when classifying packets observed by sensors installed in Japan by destination port, the daily increases and decreases in packet counts are shown separately for ranks 1–5 and 6–10 in Figure 3.1 and Figure 3.2.

The most frequently observed packets this quarter were communications to 23/TCP (Telnet), with a temporary increase for about two weeks from early January 2026. 443/TCP ranked second. 22/TCP ranked third and 80/TCP ranked fourth, swapping positions from the previous quarter. 8080/TCP ranked fifth.

[*1] Packets observed only temporarily on specific sensors, such as those from DDoS attacks, are excluded from the aggregation as they fall outside the above purpose.

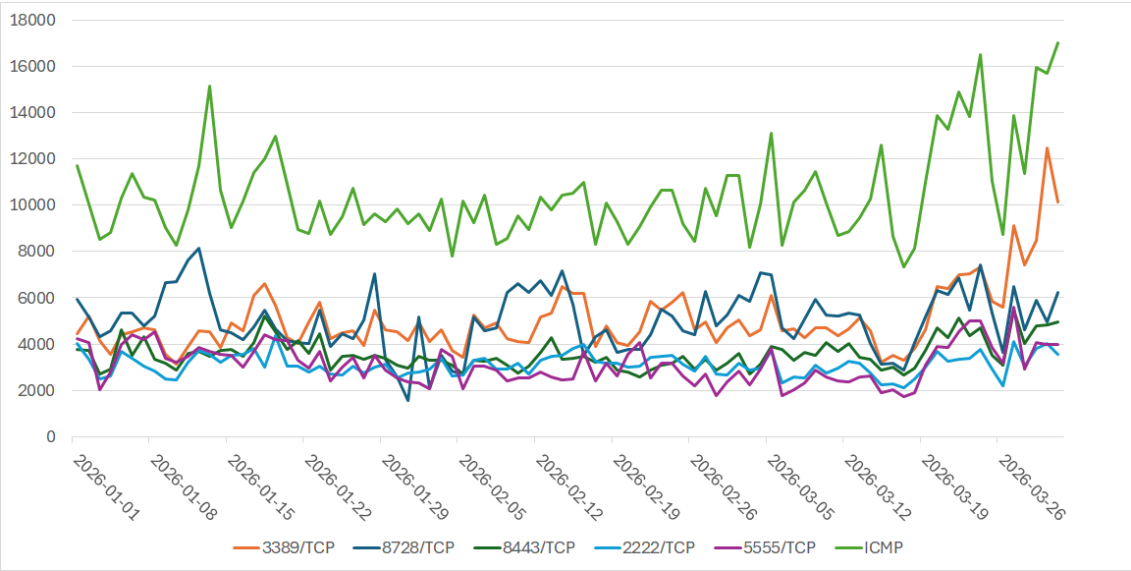

Figure 3.2 Packet Counts for Top-Ranked Destination Ports 6–10 Observed by TSUBAME (January 1, 2026–March 31, 2026)

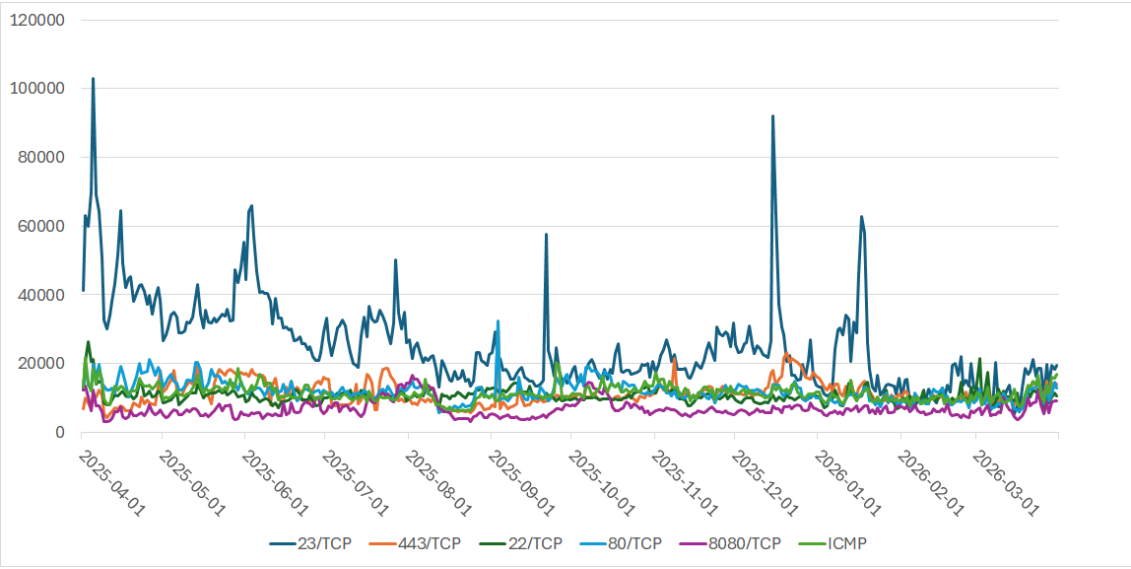

Figure 3.3 Packet Counts for Top-Ranked Destination Ports 1–5 Observed by TSUBAME (April 1, 2025–March 31, 2026)

Trends over the past year (April 1, 2025–March 31, 2026) for packet counts by destination port for ranks 1–5 and 6–10 are shown in Figure 3.3 and Figure 3.4.

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 to collect various communications sent by attackers, and analyzes attack activities together with TSUBAME observation results.

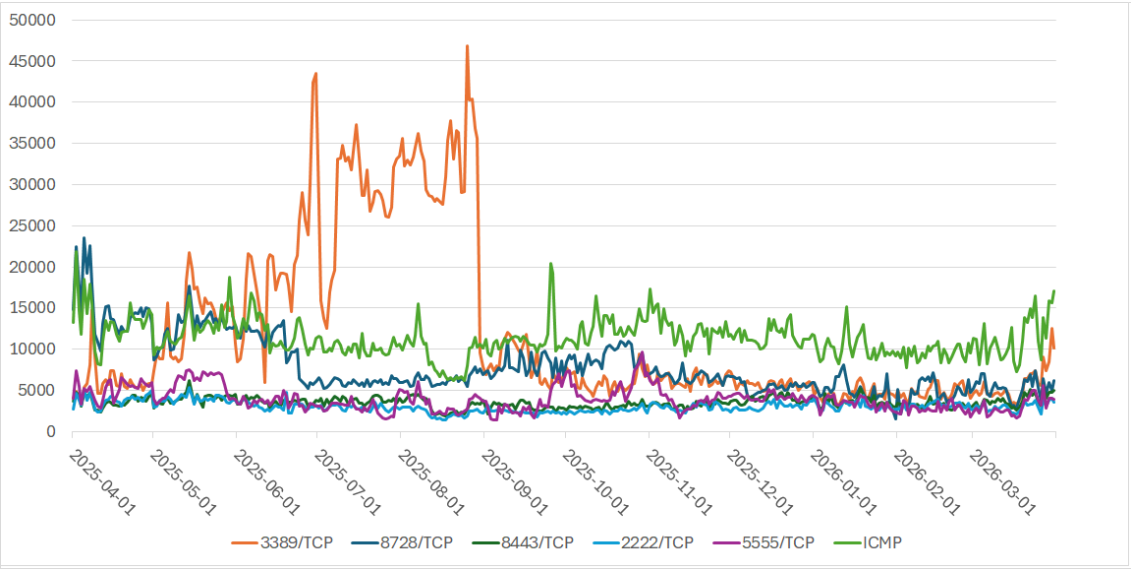

Figure 3.4 Packet Counts for Top-Ranked Destination Ports 6–10 Observed by TSUBAME (April 1, 2025–March 31, 2026)

3.2.1 Observation of Attack Activity Targeting a Vulnerability in React Server Components (CVE-2025-55182)

Attack packets targeting a vulnerability in React Server Components (CVE-2025-55182), which was published on December 3, 2025, have been continuously observed since immediately after publication (Figure 3.5).

The attack code contained in the payloads of the communications initially observed was relatively simple and intended to download malware using the wget command. However, since around mid-January 2026, more complex attack code has been observed, including code that stops other processes and persistence processing. Attack activity exploiting this vulnerability is likely to continue, and continued caution is required.

Regarding the sharp increase in the number of packets observed from February 16, 2026, to March 19, 2026, JPCERT/CC analyzes that it was caused by a large number of scan packets using existing PoC code being sent from a specific source, and does not indicate a substantial increase in attack activity.

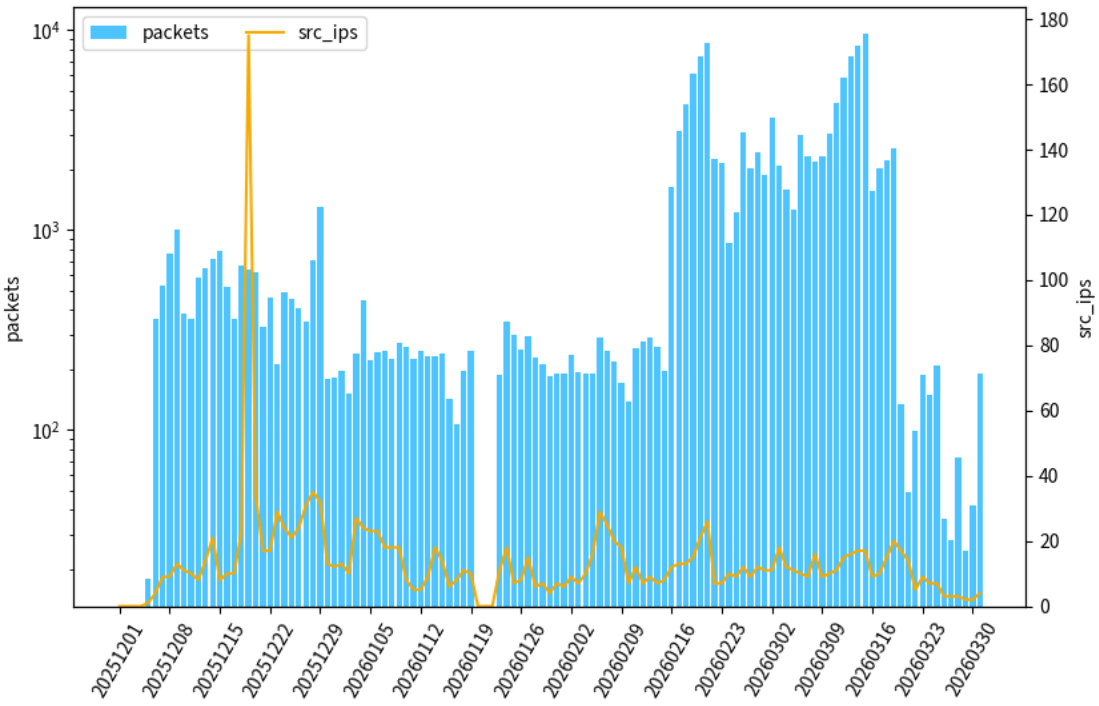

Figure 3.5 Number of Observations of Attack Activity Targeting CVE-2025-55182 (December 1, 2025 – March 31, 2026)

Chapter 4

Coordination and Dissemination of Vulnerability-Related Information

To ensure 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 and countermeasure 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 and addressing issues related to 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 we receive, we identify the relevant product developers, contact appropriate points of contact for vulnerability-related information, coordinate toward verification and remediation by product developers, and publish vulnerability information, etc. through JVN. In addition, to enable international and effective dissemination of published vulnerability information, we participate in the CVE (Common Vulnerabilities and Exposures) Program. The CVE Program is an international initiative that has been undertaken by the expert community since 1999, with the mission of identifying, describing, and cataloging published individual vulnerabilities. MITRE in the United States serves as the secretariat. Within the CVE Program, JPCERT/CC serves as a Root that oversees subordinate CNAs (CVE Numbering Authorities) and also assigns CVE IDs itself as a CNA.

As a “Coordination Organization” based on the Ministry of Economy, Trade and Industry (METI) Notification “Standards for Handling Software Vulnerability Information and Others” (METI Public Notice No. 19 of 2017, last amended by METI Public Notice No. 93 of 2024), JPCERT/CC coordinates with product developers. As a Coordination Body, activities are conducted in close

collaboration with IPA, the “Contact Organization” for vulnerability information, in accordance with the Information Security Early Warning Partnership Guideline (hereinafter the “Partnership Guideline”), which specifies the details of this standard.

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 inside and outside Japan.

4.1.2 Vulnerability Information and Response Status Published on Japan Vulnerability Notes (JVN)

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, or overseas coordination bodies without going through the Partnership Guideline (assigned an identifier in the format “JVNVU#” followed by 8 digits; e.g., JVNVU#12345678)
- Information beyond the scope of 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, 168 vulnerability advisories were published on JVN, bringing the cumulative total to 6,307; the cumulative trend is shown in Figure 4.1.

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

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

The breakdown of the vulnerability information published this quarter is as follows.

- Items related to vulnerability information reported based on the Partnership Guideline: 47
- Items related to vulnerability information through international or independent coordination: 119
- Items related to technical information associated with vulnerability information: 2

For the quarterly status of reports concerning vulnerability-related information based on the Partnership Guideline, please refer to the following web page.

- Information-technology Promotion Agency, Japan (IPA): Status of Reports Concerning

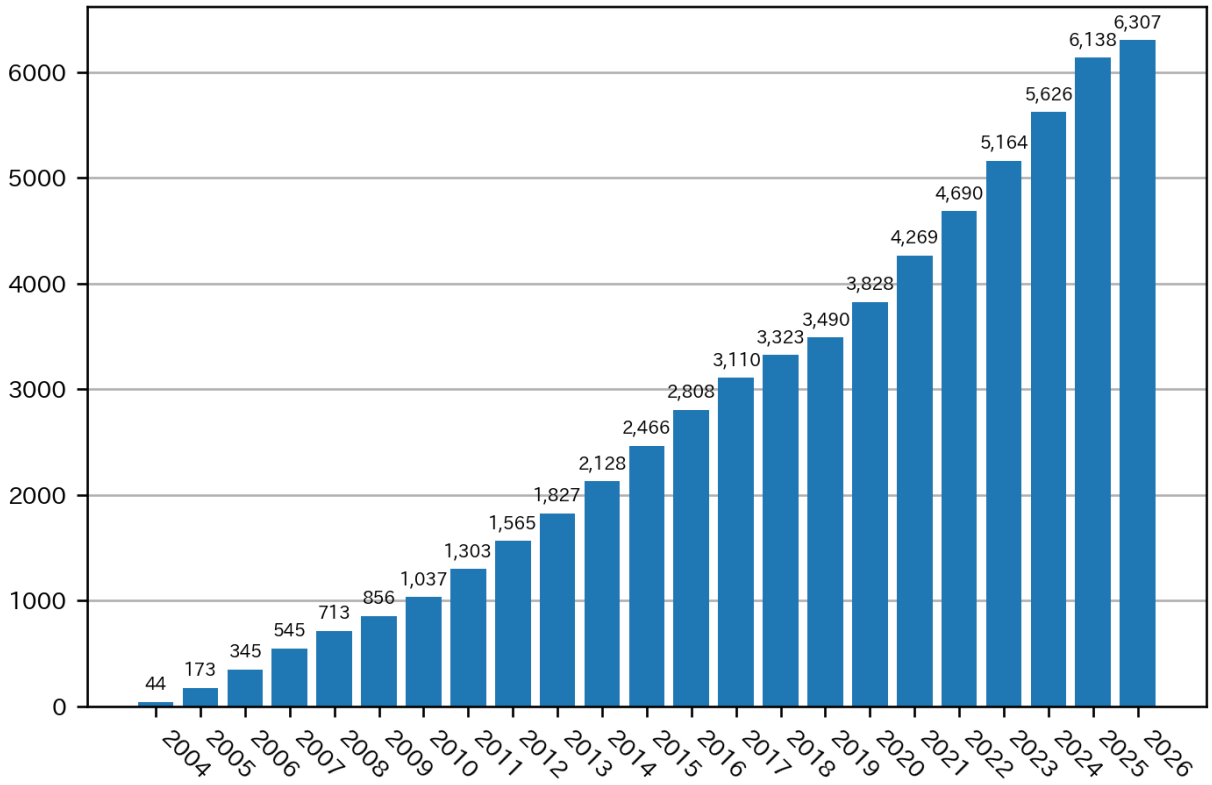

Figure 4.1 Cumulative Number of JVN Publications

Vulnerability-related Information for Software, etc.
https://www.ipa.go.jp/security/reports/vuln/software/index.html

4.1.2.1 Notable Vulnerabilities Reported Based on the Partnership Guideline

Among the vulnerabilities published this quarter that were reported based on the Partnership Guideline, we introduce noteworthy cases.

- JVN#84622767
  OS Command Injection Vulnerability in FileZen
  https://jvn.jp/jp/JVN84622767/

This is a vulnerability in "FileZen," a dedicated file transfer appliance provided by Soliton Systems K.K. This product is used by organizations in Japan, including public institutions and critical infrastructure organizations. This vulnerability was reported by the product developer as a vulnerability discovered in its own product. The vulnerability allows an attacker to execute arbitrary commands on the OS on which the product runs by sending a crafted HTTP request. If the vulnerability is exploited, it could have a serious impact on confidentiality, integrity, and availability, and it cannot be ruled out that this could lead not only to confusion among users but also to more significant damage. During coordination with the product developer, it was found that this vulnerability had

already been exploited in product users' environments. Therefore, when publishing the JVN advisory, we marked the title as "Urgent" and stated in the details that exploitation had been confirmed, urging organizations to respond promptly. After publishing the advisory, we also issued a Security Alert as an alert related to this matter to call for further caution among users. For details on this matter, please refer to 2.1.6.

4.1.2.2 Notable Vulnerabilities Handled via International or Independent Coordination

- JVNVU#95177764
  Improper Privilege Configuration Vulnerability in iRMC S5/S6 Installed on PRIMERGY
  https://jvn.jp/vu/JVNVU95177764/

This vulnerability affects the remote management module iRMC S5/S6 installed on the PRIMERGY server products provided by Fsas Technologies Inc. If this vulnerability is exploited, users assigned privileges other than "administrator" may be able to use the Redfish API beyond their privilege level or access the WebUI. Because MITRE assigned a CVE ID to this vulnerability and disclosed information about it, JPCERT/CC coordinated with the product developer to circulate the vulnerability information to users in Japan, taking into account the possibility that it could affect domestic products. At the stage when the CVE ID and related information were disclosed, the PSIRT in Japan, which serves as the contact point for coordination with JPCERT/CC, was not aware that this vulnerability had been published. Subsequently, after confirmation by the product developer, it was found that this vulnerability affected products used in Japan, so this advisory was published. As in this case, vulnerabilities in products used in Japan are sometimes disclosed without the domestic product developer being aware of them, and information cannot be provided to domestic users. To prevent such situations, product developers need to standardize their vulnerability disclosure processes in cooperation not only within Japan but also with overseas branches, affiliated companies, etc., and control the content and timing of public information disclosure across the entire company. JPCERT/CC also independently monitors newly issued CVE IDs and works with domestic product developers to ensure that necessary information reaches product users through the publication of advisories on JVN.

4.1.3 Handling of Unreachable Developers

For vulnerabilities reported under the Partnership Guideline, there are cases where we are unable to contact the product developer. In such cases, we follow the procedure for publishing cases involving unreachable developers (announced in May 2014; guideline revision). Under this procedure, the Publication Review Committee deliberates, and a decision is made on whether publication is appropriate. Based on this procedure, JPCERT/CC publishes the "List of Unreachable Developers" and the "Japan Vulnerability Notes JP (Unreachable) List" on JVN. This quarter, there were zero new publications in both.

- List of Unreachable Developers: A list intended to widely solicit contact information for the relevant product developer names
  https://jvn.jp/reply/
- Japan Vulnerability Notes JP (Unreachable) List: A list intended to inform product users of vulnerabilities deemed appropriate for publication by the Publication Review Committee
  https://jvn.jp/adj/

4.1.4 Activities as a CNA and Root

JPCERT/CC participates in the CVE Program and, as a CNA, assigns CVE IDs and, as a Root, conducts 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. This quarter, we assigned CVE IDs to 63 vulnerabilities.

For CNAs 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 Development of a Vulnerability Information Distribution Framework in Japan

JPCERT/CC has developed a vulnerability information distribution framework.

For details, please refer to the following web page.

- Vulnerability Information Handling Framework
  https://www.meti.go.jp/policy/netsecurity/vulinfo.html
- What Is Vulnerability Information Handling?
  https://www.jpcert.or.jp/vh/
- Information Security Early Warning Partnership Guideline (2024 Edition)
  https://www.jpcert.or.jp/vh/partnership_guideline2024.pdf
- JPCERT/CC Guideline for Handling Vulnerability Information (2019 Edition)
  https://www.jpcert.or.jp/vh/vul-guideline2019.pdf

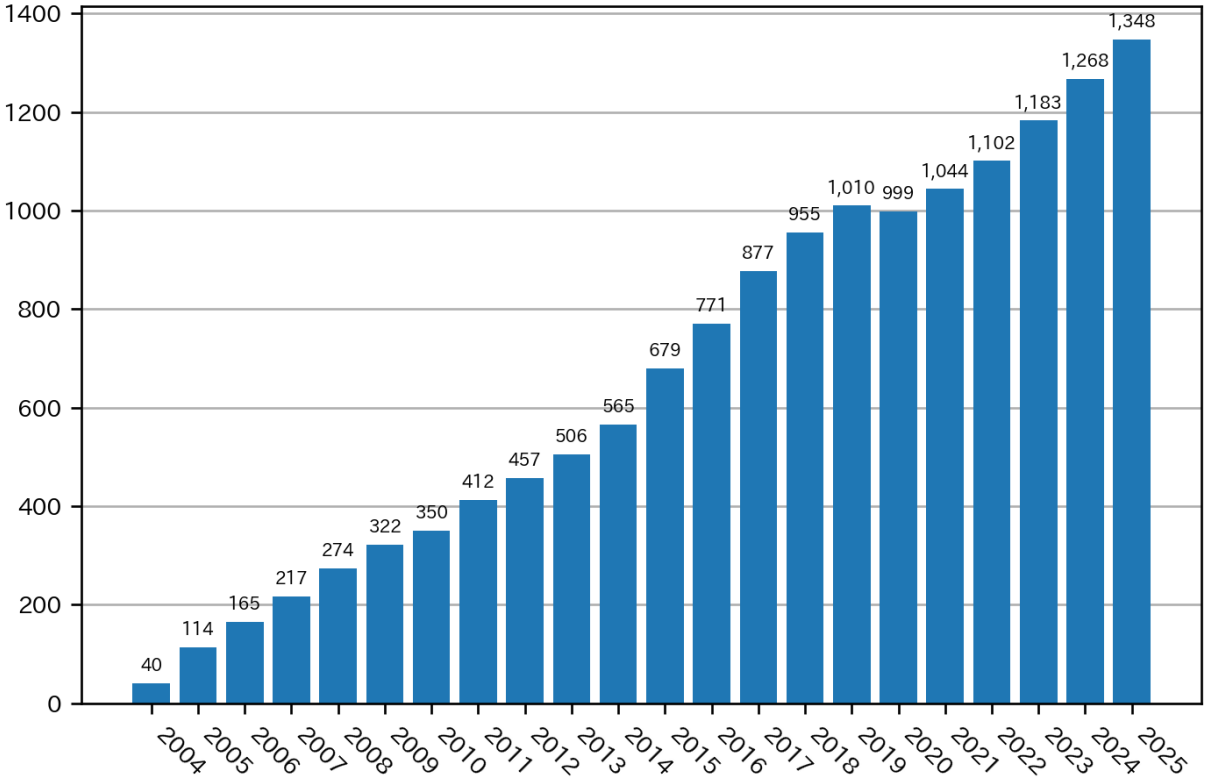

Figure 4.2 Number of Registered Product Developers

4.2.1 Collaboration with Product Developers in Japan

As a coordination center, JPCERT/CC maintains a list of product developers who are recipients of vulnerability information. We ask product developers to register, and as of the end of this quarter, the number of registrations was 1,348, as shown in Figure 4.2.

For details, please refer to the following web page.

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

4.2.2 Regular Meetings with Product Developers, etc.

This quarter, on March 13, 2026, JPCERT/CC held a regular meeting for all registered product developer vendors. The meeting was held in a hybrid format with an on-site venue and online streaming, and the total number of participants exceeded 90. The agenda covered a wide range of topics, including a guide for PSIRTs on acceptance and non-acceptance of vulnerability reports, examples of PSIRT activities by product developers, vulnerability response initiatives in the control system security personnel community, and changes to the style of publication on JVN regarding CISA ICS Advisories. Participants also exchanged opinions.

Chapter 5

Domestic Collaboration Activities

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

5.1 Collaboration with Industry Associations and Communities

We participated in gatherings hosted by organizations such as ISACs and CEPTOARs in various industries working on cybersecurity, as well as industry associations and academic societies, where we exchanged views and gave presentations. This quarter, we conducted the following activities.

5.1.1 Transportation ISAC JAPAN

We participated in the 3rd Transportation ISAC JAPAN Conference held on January 19, 2026, and gave a presentation titled "Initiatives to Address Cyber Threats and Information Sharing."

5.1.2 Japan Foreign Trade Council ISAC

We participated in the Joint Working Group held on February 20, 2026, and gave a presentation titled "Efforts to Improve Cybersecurity Across the Entire Supply Chain and Legal Issues."

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

We participated in the Security Research Joint Working Group 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 views with experts on control system security.

5.1.4 CEPTOAR Council Steering Committee

JPCERT/CC participated in the CEPTOAR Council's activities, supported Working Group activities and provided information, and jointly with the National Cybersecurity Office (NCO) supported the secretariat of the CEPTOAR Council. This quarter, at the 83rd CEPTOAR Council Steering Committee held on March 9, 2026, we shared information about the status of attack activities that exploit vulnerabilities in Cisco Catalyst SD-WAN Controller/Manager.

5.2 Strengthening Collaboration and Establishing Information Exchange Environments 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 offer opportunities for information sharing and opinion exchange. We promote interaction among organizations by holding in-person meetings, and we also invite presentations from registered organizations to stimulate dialogue.

Note that this quarter, four new organizations registered as CISTA users.

5.2.2 Working Group for Control System Security Personnel in the Manufacturing Industry

JPCERT/CC operates a Working Group of control system security personnel, primarily in the manufacturing industry. In this group, JPCERT/CC and practitioners from registered organizations collaborate to conduct practical studies on common issues related to control system security.

As of the end of this quarter, 37 organizations were registered.

5.3 Provision of Information and Tools

5.3.1 Provision of Self-assessment Tools for Control System Security

JPCERT/CC provides free of charge simple security self-assessment tools—the Japan edition SSAT (SCADA Self Assessment Tool; application required) and J-CLICS (Industrial Control System Security Self-assessment Tool)—with the aim of identifying security issues related to the construction and operation of control systems and enabling well-balanced security measures.

- Japan Edition 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: Countermeasures for Attack Paths (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 that JPCERT/CC handles require information sharing and collaboration with CSIRTs, ISPs, and government agencies in other countries. Therefore, JPCERT/CC identifies trusted counterparts in each country before incidents occur and builds relationships of trust to enable mutual cooperation when necessary. In this chapter, we present notable outcomes of such international cooperation activities.

6.1 Support for Building and Operating Overseas CSIRTs

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

6.2 International CSIRT Collaboration

We actively participate in multilateral CSIRT collaboration frameworks, such as playing a leading role in APCERT and FIRST.

6.2.1 APCERT (Asia Pacific Computer Emergency Response Team)

APCERT is a CSIRT community in the Asia-Pacific region established in February 2003. Since its establishment, JPCERT/CC has continuously been elected as a member of the Steering Committee and has also served as its Secretariat.

For details about APCERT and JPCERT/CC's role in 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 February 5, 2026, to discuss APCERT's operational policies and other matters. JPCERT/CC participated in the meetings as a Steering Committee member and also supported meeting operations as the Secretariat.

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 of the Global Coordination Division has served on the Board and this quarter participated in the monthly online Board meetings, as well as the in-person Board meeting held in the Dominican Republic in January 2026.

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

6.3 Visits to and from Overseas CSIRTs, etc.

Through visits to and from overseas CSIRTs, JPCERT/CC discusses with them and exchanges views on future collaboration. This quarter, we visited the following organizations. (See Figure 6.1 and Figure 6.2.)

- Visit to CERT-EU (January 29, 2026)
- Visit to CERT.AZ in Azerbaijan (March 2, 2026)
- Visit to CERT.GOV.AZ in Azerbaijan (March 3, 2026)

6.4 Participation in Other International Conferences

6.4.1 Panel Participation at Tallinn Cyber Diplomacy Winter School 2026

JPCERT/CC participated in Tallinn Cyber Diplomacy Winter School 2026, held in Bangkok, Thailand, on March 2, 2026. This conference is held annually with the primary participation of diplomats and policymakers from various countries, with the aim of cooperating on and promoting cyber diplomacy and international collaboration. JPCERT/CC joined a panel session on cyber threats and spoke about the latest attack cases, the role of CERTs in incident response, and international collaboration among CERTs.

Figure 6.1 Photo from the Visit to CERT.AZ

Figure 6.2 Photo from the Visit to CERT.GOV.AZ

- Tallinn Cyber Diplomacy Winter School 2026
  https://cyberdiplomacy.ee/wp-content/uploads/2026/03/winter-school-2026-agenda.pdf

6.5 International Standardization Activities

Among the standardization activities underway in ISO/IEC JTC 1/SC 27, an organization for standardization in the IT security field, we participated via the Information Technology Standards Commission of Japan in part of the standardization work being considered in Working Group 3 (responsible for standardization of security evaluation, testing, and specification) and in the revision of the standard on incident management being considered in Working Group 4 (responsible for standardization of security controls and services).

This quarter, a meeting related to WG3 was held in Nuremberg, Germany, in March 2026. Regarding the Working Drafts for both ISO/IEC 29147 (Vulnerability disclosure) and 30111 (Vulnerability handling processes), which were under revision, major points of discussion included the definition of vulnerability, consistency with other documents, and decisions on requirements and recommendations in vulnerability response. JPCERT/CC participated as a main editor and discussed how to handle comments from experts in each country. As a result, it was decided to revise the Working Drafts and prepare second editions by June. The major points of discussion this time included the definition of vulnerability, consistency with other documents, and decisions on requirements and recommendations in vulnerability response.

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. JPCERT/CC, commissioned by the Ministry of Economy, Trade and Industry, handles acceptance of phishing reports and inquiries from general consumers, publishes Security Alerts about phishing sites, and operates certain working groups as part of the Council's activities.

In addition, the Council reports phishing sites reported to it to JPCERT/CC, and in response, JPCERT/CC conducts coordination to take down phishing sites as part of its incident response support activities.

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

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

7.1 Operation of the Secretariat of the Council of Anti-Phishing Japan

7.1.1 Acceptance of Phishing Reports and Inquiries

Although the figure for this quarter has not yet been finalized, the number of phishing reports has decreased significantly. In past years, reports of phishing emails originating from .cn domains have tended to decrease during the Lunar New Year period, but this quarter saw a larger decrease than usual. One possible factor behind this is the neutralization[*1] of the world's largest residential

[*1] "No Place Like Home Network: Disrupting the World's Largest Residential Proxy Network" https://cloud.google.com/blog/topics/threat-intelligence/disrupting-largest-residential-proxy-network?hl=en

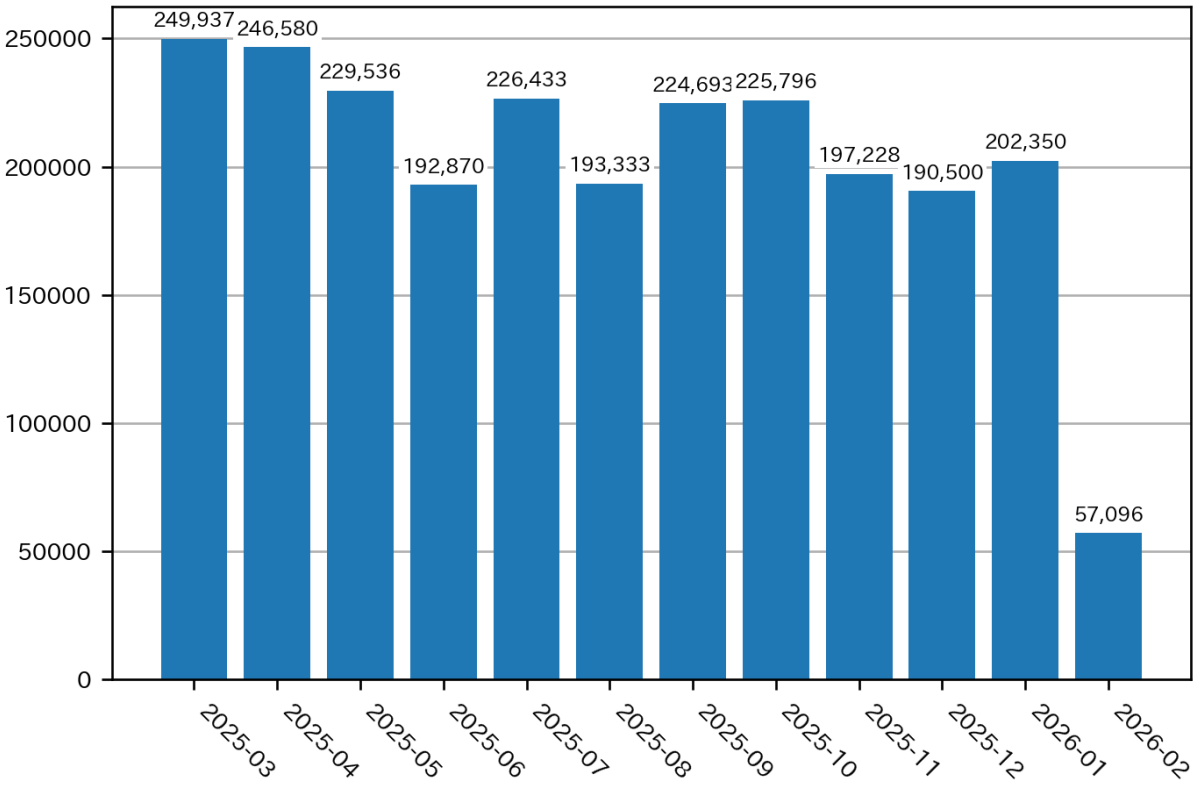

Figure 7.1 Number of Phishing Reports

proxy[*2] network carried out by Google around the end of January.

The trend in the number of phishing reports over the past year is shown in Figure 7.1.

By breakdown of reports, those impersonating Amazon were the most numerous, accounting for about 16.2% of the total. This was followed by reports of phishing impersonating Monex, Inc., accounting for about 7.9% of the total.

7.1.2 Information Gathering and Distribution

7.1.2.1 Regular Reports

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/
- 2025/12 Phishing Report Status

[*2] A proxy that uses smartphones, PCs, IoT devices, and other devices connected to home networks as relay points to communicate via residential IP addresses. Because the traffic appears to be from general users, it is difficult to detect and can be abused by criminals for unauthorized access, fraud, and other purposes.

https://www.antiphishing.jp/report/monthly/202512.html

- 2026/01 Phishing Report Status
  https://www.antiphishing.jp/report/monthly/202601.html
- 2026/02 Phishing Report Status
  https://www.antiphishing.jp/report/monthly/202602.html

7.1.2.2 Provision of Phishing Site URL Information

We provide Council member organizations, such as vendors that offer phishing countermeasure toolbars and antivirus software and academic institutions conducting phishing-related research, with a list of URLs of phishing sites reported to the Council. This aims to strengthen anti-phishing products and promote related research. As of the end of this quarter, we were providing information to 51 organizations and plan to continue providing it broadly upon request.

7.2 Activities for Member Organizations of the Council of Anti-Phishing Japan

As the Secretariat, JPCERT/CC supported the following independent activities for member organizations conducted based on decisions of the Steering Committee.

7.2.1 Steering Committee Meetings

This quarter, we held the Steering Committee, which plans activities and determines operating policies for the Council, as follows.

- 135th Steering Committee (Online)
  Date: February 26, 2026, 16:00–18:00
- 136th Steering Committee (JPCERT/CC Conference Room + Online)
  Date: March 26, 2026, 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: Every Tuesday from January 2026 to March 2026, 9:00–9:30 (Online)
- Technical and Institutional Study Working Group Meeting
  Date: January 29, 2026, 16:00–18:00 (JPCERT/CC Conference Room + Online)
  Same Working Group Results Briefing
  Date: February 25, 2026, 17:00–19:00 Results Briefing (TKP Akihabara Conference Center

Conference Room 2A + Online)

- Certificate Promotion Working Group Meeting
  Date: February 16, 2026, 16:00–17:30 (Online)
- Fake Site Response Automation Task Force Meeting
  Date: January 30, 2026, 11:00–11:30 (Online)
  Date: February 20, 2026, 11:30–12:00 (Online)
  Date: March 17, 2026, 10:30–11:00 (Online)
- 12th Anti-Phishing Workshop
  Date: January 28, 2026, 17:00–20:00 (Japan Cybercrime Control Center Conference Room)

Chapter 8

Public Relations Activities

JPCERT/CC conducts broad public relations regarding our business outcomes and strives to disseminate and raise awareness of the results. We distribute information via the JPCERT/CC website and X (formerly Twitter), as well as through various media such as online media, broadcast media, and print media. We also share information by speaking at seminars and events.

8.1 Presentations

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

- Cyber Tech Talk
  Title: Structure of Repeated Edge Device Compromises
  Presenter: Yusuke Tsukada (Threat Information Analyst, Early Warning Group)
  Organizer: SOMPO Holdings, Inc.
  Presentation date: January 19, 2026
- ISAJ Technical Forum - OT Cybersecurity and Plant AI Applications
  Title: Current State and Outlook for Control System Security: Looking Back on the Past Year
  Presenter: Toshio Miyachi (Technical Advisor)
  Organizer: ISA Japan Section
  Presentation date: February 19, 2026
- FY2025 Boiler and Turbine Chief Engineers Meeting
  Title: Cyberattack Threats in the Electric Power Industry and JPCERT/CC Initiatives
  Presenter: Nobukatsu Toudou (Threat Information Analyst, Early Warning Group)
  Organizer: Chugoku-Shikoku Industrial Safety and Inspection Department, Ministry of Economy, Trade and Industry
  Presentation Date: February 27, 2026
- [JPCERT/CC Presentation] Introduction to Secure Development for Embedded and Control Systems

Title: Basics of Secure Development in Embedded and Control Systems
Presenter: Hiromi Kinoshita (Vulnerability Analyst, Early Warning Group)
Organizer: TechMatrix
Presentation date: March 10, 2026

- Security Camp 2026 Connect
  Title: Understanding Threats in Cyberspace
  Presenter: Hayato Sasaki (General Manager of Strategy and Early Warning Group Manager, Threat Analyst)
  Organizer: Information-technology Promotion Agency, Japan (IPA)
  Presentation date: March 27, 2026

8.2 Publications

This quarter, we contributed to the following publications and websites.

- Internet White Paper 2026
  Title: Information Security Trends in 2025
  Author: Ryosuke Shiraishi (Threat Analyst, Early Warning Group)
  Publisher: Impress Corporation
  Publication date: February 27, 2026

8.3 Support and Sponsorship

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

- Campaign to Promote Replacement of Routers No Longer Under Maintenance
  Organizer: The Japan Internet Providers Association, Digital Life Promotion Association
  Event dates: February 1, 2026–March 18, 2026
- Security Days Spring 2026
  Organizer: NANO OPT Media
  Event dates: March 10, 2026–March 27, 2026
- Security Management Conference Spring 2026
  Organizer: SB Creative
  Event dates: March 11, 2026 - March 12, 2026
- Data Center Japan 2026
  Organizer: NANO OPT Media
  Event dates: March 24, 2026–March 25, 2026

8.4 Published Materials

This quarter, we published the following materials.

8.4.1 Internet Threat Monitoring Report

JPCERT/CC has built and continues to operate TSUBAME, an Internet threat monitoring system that distributes multiple monitoring sensors across the Internet and continuously collects packets sent to a large number of unspecified hosts. By classifying packets observed by the sensors and analyzing them against vulnerability information and information on malware and attack tools, we have worked to capture attack activities and their preparatory activities. We compile the results of such Internet monitoring each quarter and publish them as reports in Japanese and English.

- 2026-03-09
  JPCERT/CC Internet Threat Monitoring Report [July 1, 2025 - September 30, 2025]
  https://www.jpcert.or.jp/tsubame/report/report202507-09.html
- 2026-03-25
  JPCERT/CC Internet Threat Monitoring Report [July 1, 2025 - September 30, 2025]
  https://www.jpcert.or.jp/english/tsubame/report/report202507-09.html
- 2026-03-09
  JPCERT/CC Internet Threat Monitoring Report [October 1, 2025 - December 31, 2025]
  https://www.jpcert.or.jp/tsubame/report/report202510-12.html
- 2026-03-25
  JPCERT/CC Internet Threat Monitoring Report [October 1, 2025 - December 31, 2025]
  https://www.jpcert.or.jp/english/tsubame/report/report202510-12.html

8.4.2 Status of Reports on Software Vulnerability-Related Information

As the receiving and coordinating organizations, respectively, IPA and JPCERT/CC have, since July 2004, undertaken part of the operation of the vulnerability information handling scheme based on the Ministry of Economy, Trade and Industry's "Standards for Handling Software Vulnerability Information and Others" (METI Public Notice No. 19 of 2017, last amended by METI Public Notice No. 93 of 2024), among others. We publish a report summarizing operational results for the previous quarter and notable trends in vulnerabilities disclosed during the same period.

- 2026-01-22
  Status of Reports on Software Vulnerability-Related Information [Q4 2025 (October–December)]
  https://www.jpcert.or.jp/pr/2026/vulnREPORT_2025q4.pdf

8.4.3 Official Blog "JPCERT/CC Eyes"

The official blog of the JPCERT Coordination Center, "JPCERT/CC Eyes," quickly delivers articles that present analyses and investigations by JPCERT/CC, as well as coverage of events and conferences in Japan and overseas, through the eyes of JPCERT/CC analysts.

This quarter, we published the following 15 articles.

Japanese edition: 8 articles https://blogs.jpcert.or.jp/ja/

- 2026-02-10
  Publication of Training Content for Windows Event Log Analysis
- 2026-02-13
  Multiple Threat Actors Rapidly Exploit React2Shell: A Case Study of Active Compromise
- 2026-02-20
  JSAC2026 -Day 1-
- 2026-02-27
  JSAC2026 -Day 2-
- 2026-03-06
  JSAC2026 -Workshop/Lightning Talk Session/Panel Discussion-
- 2026-03-24
  ICS Security Conference 2026
- 2026-03-25
  CSIRTs Around the World – Azerbaijan
- 2026-03-30
  TSUBAME Report Overflow (Jul–Sep 2025)

English edition: 7 articles https://blogs.jpcert.or.jp/en/

- 2026-02-13
  Multiple Threat Actors Rapidly Exploit React2Shell: A Case Study of Active Compromise
- 2026-02-20
  JSAC2026 -Day 1-
- 2026-02-27
  JSAC2026 -Day 2-
- 2026-03-06
  JSAC2026 -Workshop/Lightning Talk Session/Panel Discussion-
- 2026-03-12
  Study of Binaries Created with Rust through Reverse Engineering
- 2026-03-25
  CSIRTs Around the World – Azerbaijan

- 2026-03-30
  TSUBAME Report Overflow (Jul-Sep 2025)

Appendix A

Incident Categories

At JPCERT/CC, incidents included in received reports are classified according to the following definitions.

Phishing Site

Phishing site refers to a site used for "phishing scams" that impersonate legitimate sites of service providers such as banks and auctions to trick users into divulging information such as IDs, passwords, and credit card numbers.
At JPCERT/CC, the following are classified as **phishing sites**.

- Websites that imitate sites of financial institutions, credit card companies, etc.
- Websites set up to lead users to phishing sites

Website Defacement

Website defacement refers to a site where the website content has been altered by an attacker or malware (including the insertion of scripts not intended by the administrator).
At JPCERT/CC, the following are classified as **website defacement**.

- Sites into which malicious scripts, iframes, etc. have been embedded by attackers or malware
- Sites where information has been altered due to SQL injection attacks

Malware Site

Malware site refers to an attack site that infects a PC with malware upon viewing, or a site that publishes malware used in attacks.
At JPCERT/CC, the following are classified as **malware sites**.

- Sites that attempt to infect visitors' PCs with malware
- Sites where attackers have published malware

Scan

Scan refers to accesses performed by attackers (that have no impact on the system) to confirm the existence of systems that may be attack targets such as servers or PCs, or to search for vulnerabilities (security holes, etc.) to illegally intrude into systems. In addition, infection activities by malware, etc. are also included.
At JPCERT/CC, the following are classified as **scans**.

- Vulnerability probing (e.g., checking program versions and service operating status)
- Attempts at intrusion (that ended in failure)
- Attempts at infection by malware (viruses, bots, worms, etc.) (that ended in failure)
- Brute-force attacks against ssh, ftp, telnet, etc. (that ended in failure)

DoS/DDoS

DoS/DDoS refers to attacks against network resources such as servers and PCs on a network, and devices and lines that constitute the network, to render services unavailable.
At JPCERT/CC, the following are classified as **DoS/DDoS**.

- Attacks that exhaust network resources through large volumes of traffic, etc.
- Degradation or stoppage of server program responses due to large volumes of access
- Service disruption caused by sending large volumes of email (bounce mail, spam mail, etc.)

Control System-related Incidents

Control system-related incidents refers to incidents related to control systems and various plants.
At JPCERT/CC, the following are classified as **control system-related incidents**.

- Control systems that can be attacked via the Internet
- Servers communicating with malware targeting control systems
- Attacks that cause abnormal operation, etc. in control systems

Targeted Attack

Targeted attack refers to an attack that targets specific organizations, companies, industries, etc., attempting malware infection or information theft.
At JPCERT/CC, the following are classified as **targeted attacks**.

- Spoofed emails sent to specific organizations with malware attached
- Defacement of websites whose viewers are limited to certain organizations
- Sites that impersonate websites whose viewers are limited to certain organizations and attempt to infect users with malware
- Servers communicating with malware targeting specific organizations

Other

Other refers to incidents not covered above.
Examples of items JPCERT/CC classifies as **other** are listed below.

- Unauthorized intrusions into systems by exploiting vulnerabilities, etc.
- Unauthorized intrusions due to successful brute-force attacks against ssh, ftp, telnet, etc.
- Information theft by malware with keylogger functionality
- Infection by malware (viruses, bots, worms, etc.)

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

- JPCERT Coordination Center (JPCERT/CC): https://www.jpcert.or.jp/
- To provide incident information or request assistance: info@jpcert.or.jp, https://www.jpcert.or.jp/form/
- Inquiries about vulnerability information handling: vultures@jpcert.or.jp
- Inquiries about control system security: dc-info@jpcert.or.jp
- Inquiries about the Secure Coding Seminar: secure-coding@jpcert.or.jp
- Inquiries about citing published materials, presentation requests, and other inquiries: pr@jpcert.or.jp
- About the PGP public key: https://www.jpcert.or.jp/jpcert-pgp.html

JPCERT/CC Quarterly Report [January 1, 2026 to March 31, 2026]

- Revision History
  - April 16, 2026 First Japanese version
  - August 21, 2026 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/