JPCERT CC®

JPCERT/CC Quarterly Report

October 1, 2025 to December 31, 2025

January 22, 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 October 1, 2025 to December 31, 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" include some descriptions of voluntary activities other than sponsored activities.

Topics & Highlights

Presentation of the JPCERT/CC Best Reporter Award for FY2025

Those who promptly discover cybersecurity issues such as incidents and vulnerabilities and provide accurate information are important sources of information and collaborators that enable JPCERT/CC to effectively proceed with coordination toward resolving issues. Given the current situation in which the number of incidents and vulnerabilities has increased and issues have become more complex and sophisticated, it has become increasingly important to quickly resolve more issues based on the information provided by reporters. In light of this situation, JPCERT/CC established the "Best Reporter Award" in FY2021 to express our gratitude for the support of reporters and to provide an opportunity to widely publicize particularly outstanding examples of activities. We have two categories—Incident Reporting and Vulnerability Reporting—and present awards to those who have made remarkable contributions to JPCERT/CC's activities based on the number and content of incident or vulnerability reports they provided.

In this fifth year, we presented the Best Reporter Award to the following recipients.

Furujukukai Medical Group, Mr. Naoya Saito (Incident Reporting Category)

Mr. Saito submitted over 500 reports on phishing emails and phishing sites targeting each facility and staff member, discovered in the course of implementing cybersecurity measures and incident response as an information system administrator for medical institutions and facilities. These reports were used for JPCERT/CC's handling of the sites, analysis, and the issuance of Security Alerts, among others.

GMO Flatt Security, Inc., RyotaK (Vulnerability Reporting Category)

RyotaK has discovered numerous product vulnerabilities and, in collaboration with product developers and coordination organizations, has greatly contributed to the appropriate dissemination of vulnerability information, demonstrating exemplary behavior for reporters in Coordinated Vulnerability Disclosure (CVD).

We would like to once again express our gratitude to the awardees and to the many individuals who support JPCERT/CC's activities on a daily basis.

- JPCERT/CC Best Reporter Award 2025
  https://www.jpcert.or.jp/award/best-reporter-award/2025.html

Release of YAMAGoya, a Real-time Client Monitoring Tool

JPCERT/CC has released YAMAGoya, an open-source threat hunting tool that enables real-time monitoring of malicious behavior on Windows endpoints by leveraging Sigma and YARA rules.

- GitHub: JPCERTCC/YAMAGoya
  https://github.com/JPCERTCC/YAMAGoya
- JPCERT/CC Eyes: YAMAGoya: A Real-time Client Monitoring Tool Using Sigma and YARA Rules
  https://blogs.jpcert.or.jp/en/2025/11/YAMAGoya.html

In recent years, due to fileless malware and malware obfuscation, detecting suspicious activity on hosts has become difficult with file-only scans. Meanwhile, although rules such as Sigma and YARA are actively created and published within the security community and their use is advancing, existing endpoint products often use proprietary detection engines, which makes it difficult to directly utilize these rules. YAMAGoya aims to support monitoring and detection that assumes the use of publicly available rules such as Sigma and YARA to address these challenges.

YAMAGoya is designed to detect by combining event monitoring via ETW (Event Tracing for Windows) with memory scanning, and it includes functions to monitor files, processes, registry, network, PowerShell, WMI, etc. It also supports both GUI and CLI, making it useful as an auxiliary tool for threat hunting and incident response.

This tool can be used for threat hunting on Windows endpoints.

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 from October 1, 2025 to December 31, 2025 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 are shown in Table 1.1[*2].

The number of reports received this quarter was 20,336. Among these, the number of cases in which JPCERT/CC coordinated with relevant organizations in Japan and overseas was 2,875. Compared to the previous quarter, the number of reports decreased by 15% and the number of cases coordinated decreased by 12%. Also, compared to the same period last year (number of reports: 9,743; number of cases coordinated: 3,597), the number of reports increased by 109% 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

	Oct	Nov	Dec	Total	Last Qtr.
Number of Reports	6,852	7,039	6,445	20,336	23,857
Number of Incidents	4,474	5,011	4,052	13,537	10,379
Cases Coordinated	1,011	799	1,065	2,875	3,257

[*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.

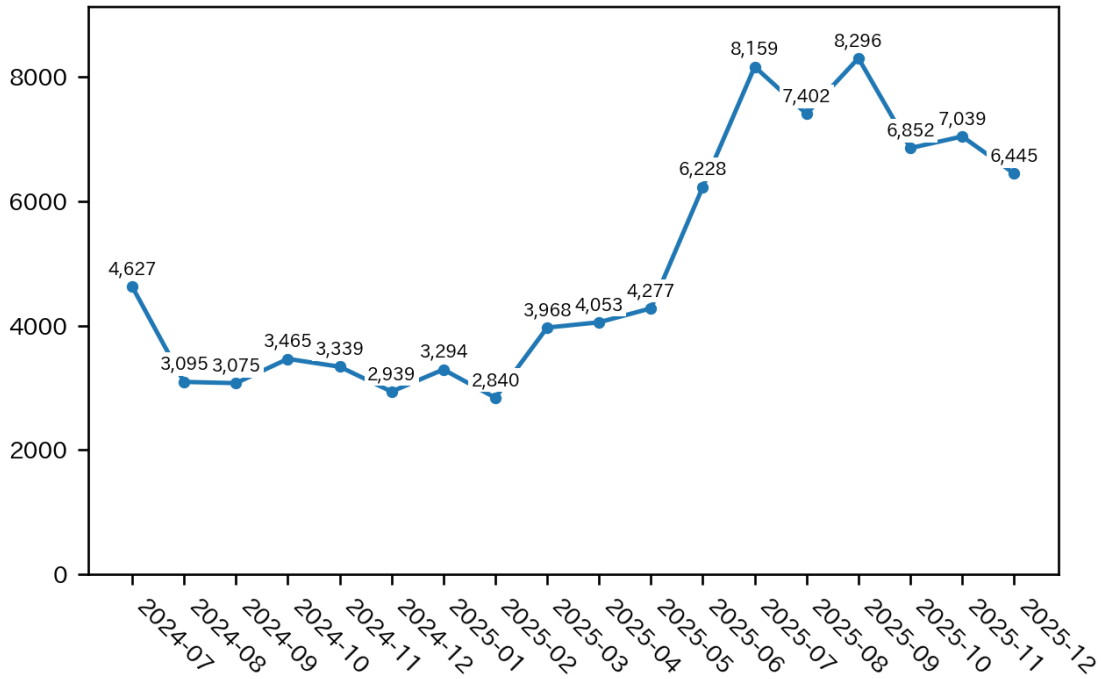

Figure 1.1 Trends in the Number of Incident Reports

Table 1.2 Number of Incident Reports by Category

Incident Category	Oct	Nov	Dec	Total	Last Qtr.
Phishing Site	4,073	4,624	3,700	12,397	9,063
Website Defacement	23	65	17	105	319
Malware Site	19	8	17	44	32
Scan	216	156	97	469	452
DoS/DDoS	2	4	0	6	2
ICS Related	0	0	0	0	0
Targeted Attack	1	0	2	3	3
Other	140	154	219	513	508

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 91.58%, and incidents classified as scans, which probe system vulnerabilities, accounted for 3.46%.

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.

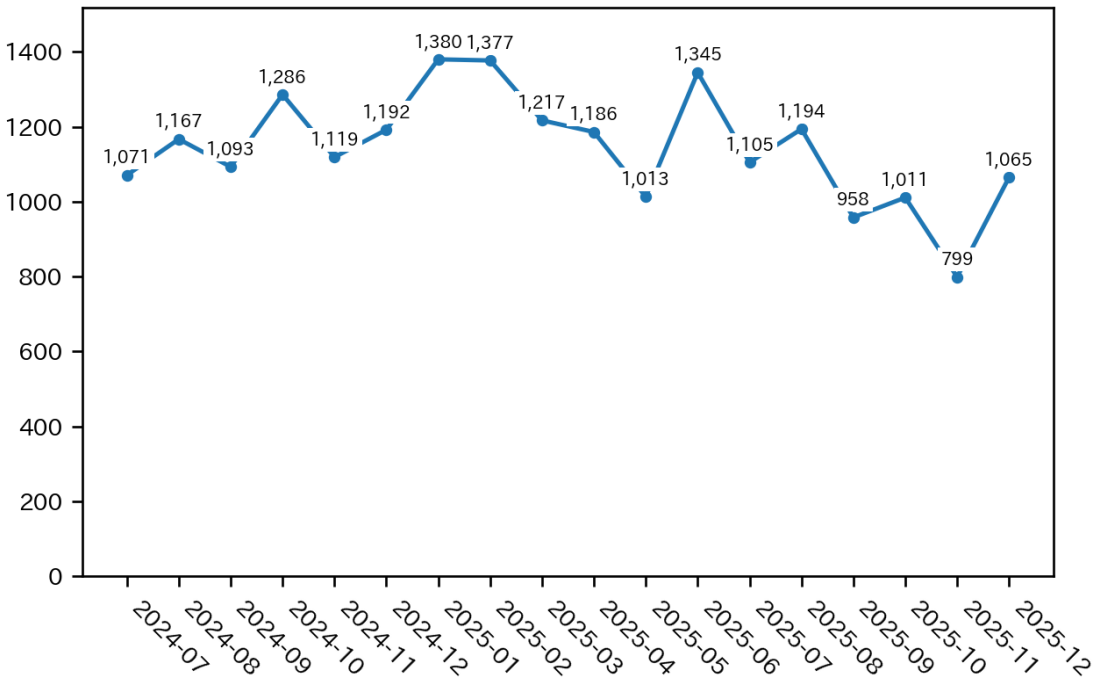

Figure 1.2 Trends in the Number of Cases Coordinated

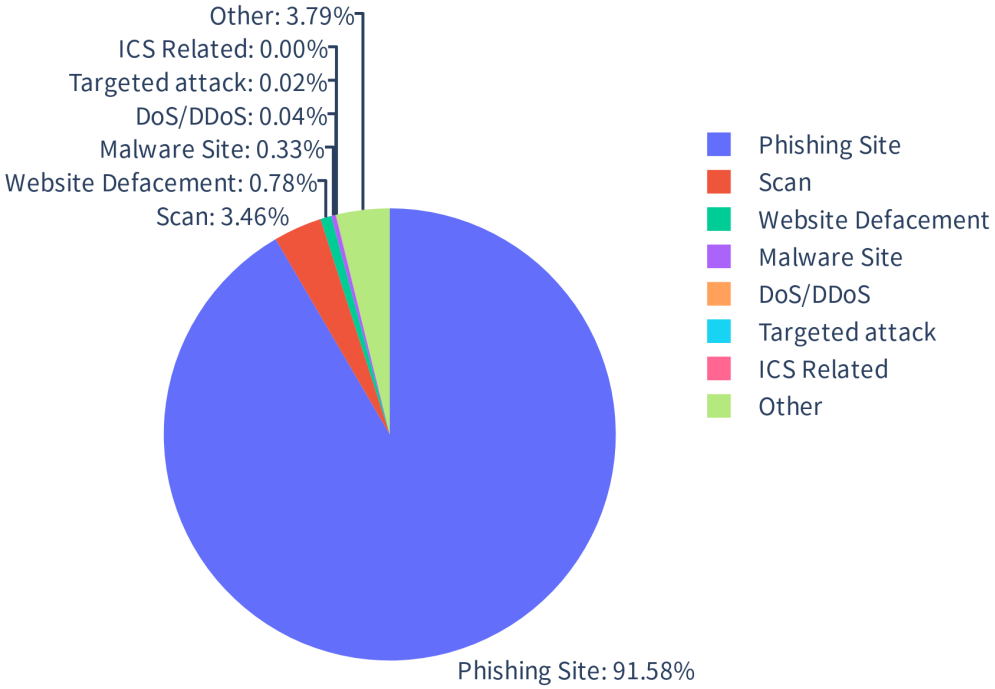

Figure 1.3 Percentage of the Number of Incident Reports by Category

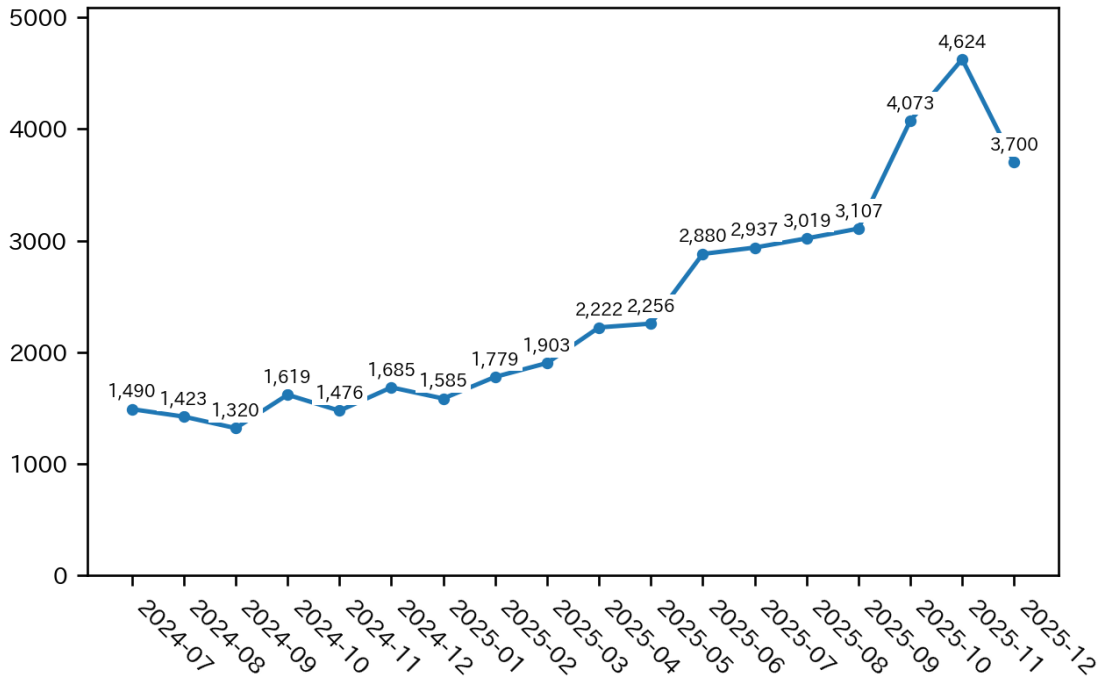

Figure 1.4 Trends in the Number of Phishing Sites

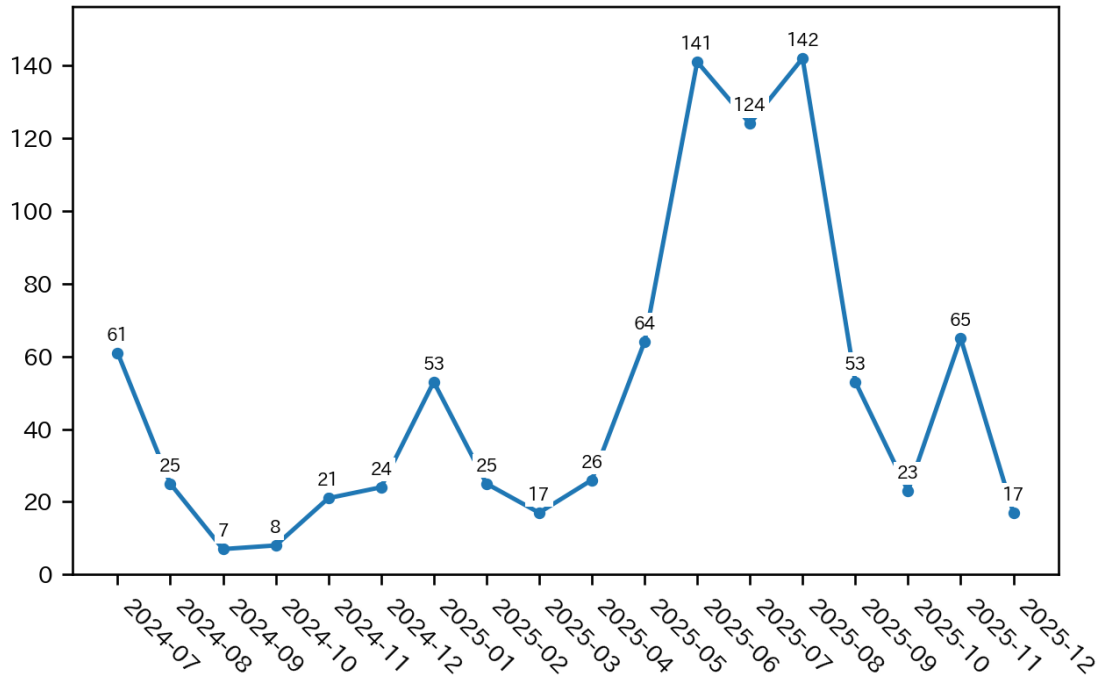

Figure 1.5 Trends in the Number of Website Defacements

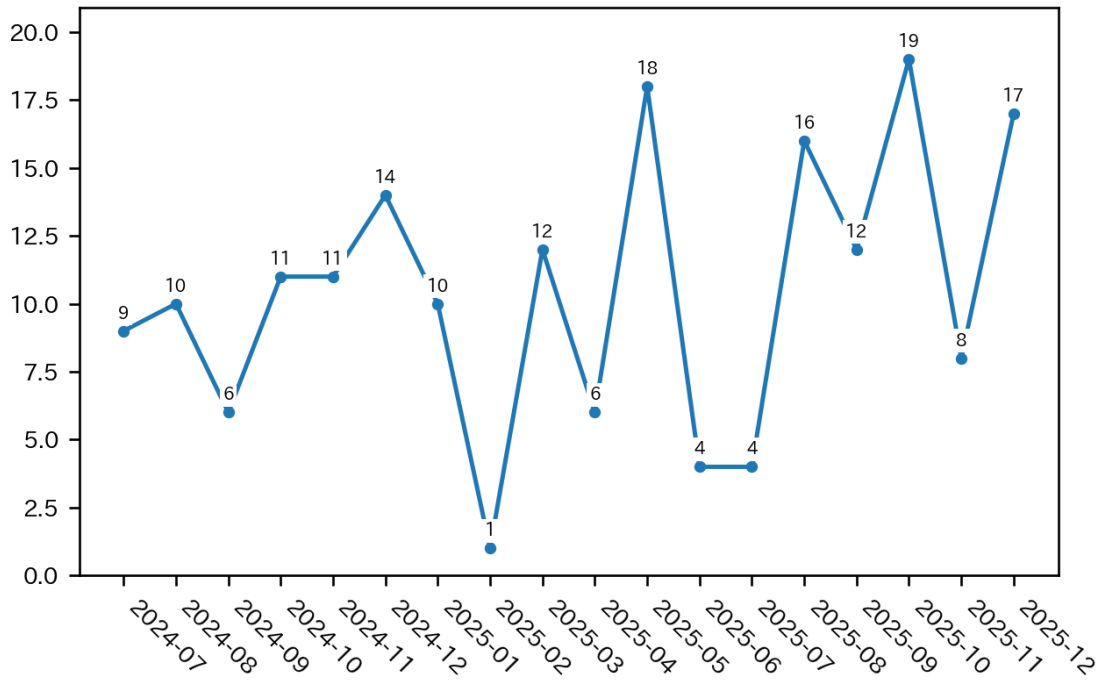

Figure 1.6 Trends in the Number of Malware Sites

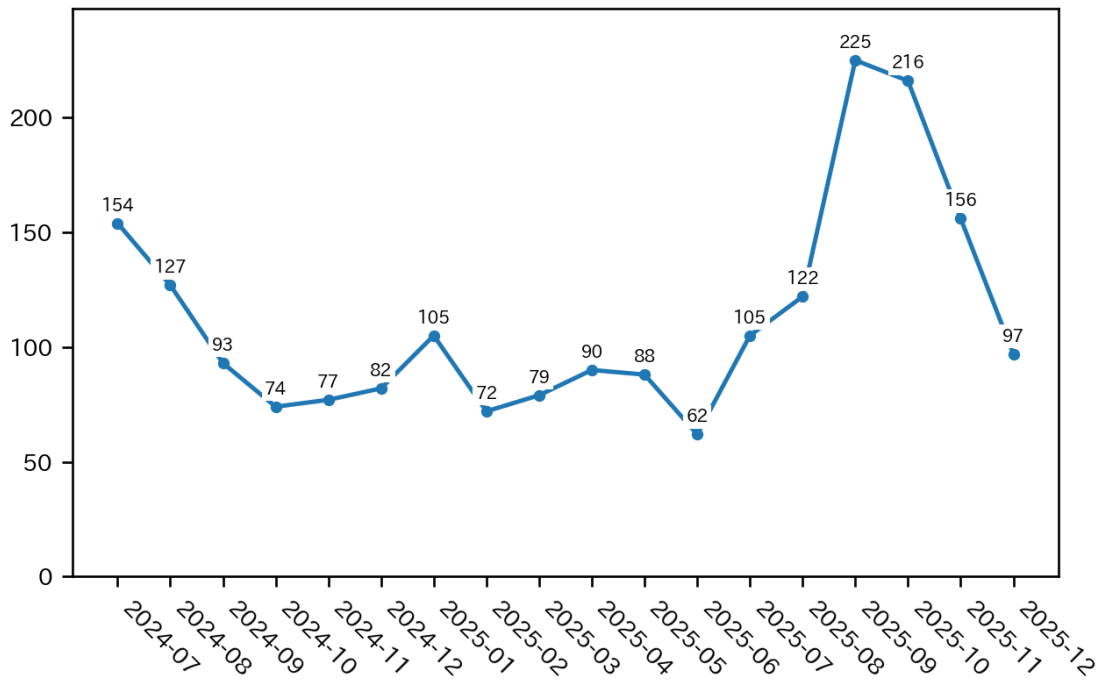

Figure 1.7 Trends in the Number of Scans

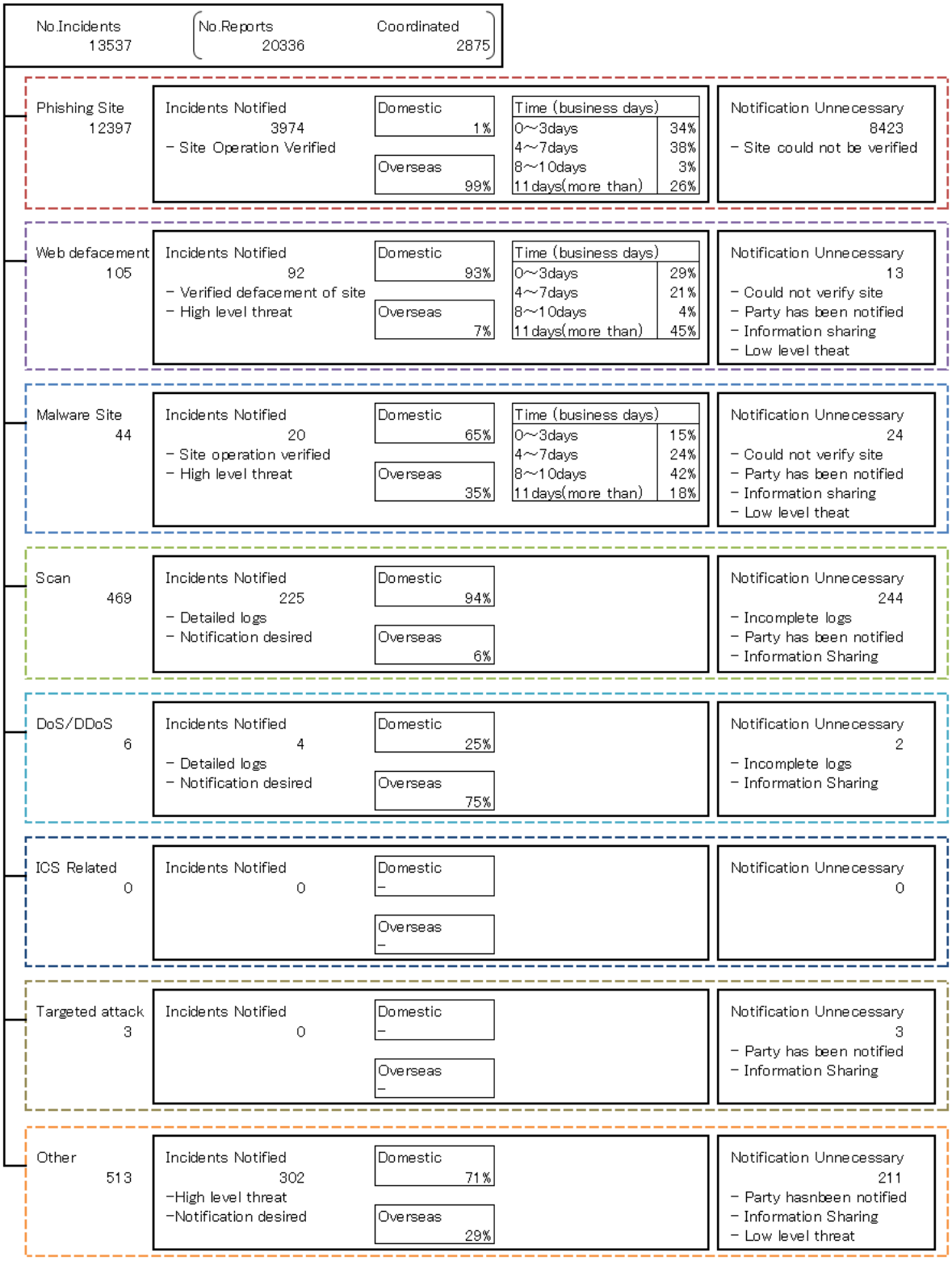

Figure 1.8 Number of Cases and Coordination/Response Status by Incident Category

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

Table 1.3 Number of Phishing Sites for Domestic and Overseas Brands

Phishing Site	Oct	Nov	Dec	Total	Pct.
Domestic Brand	3,349	4,068	3,115	10,532	85%
Overseas Brand	225	144	200	569	5%
Unknown Brand	499	412	385	1,296	10%
Monthly Total	4,073	4,624	3,700	12,397	

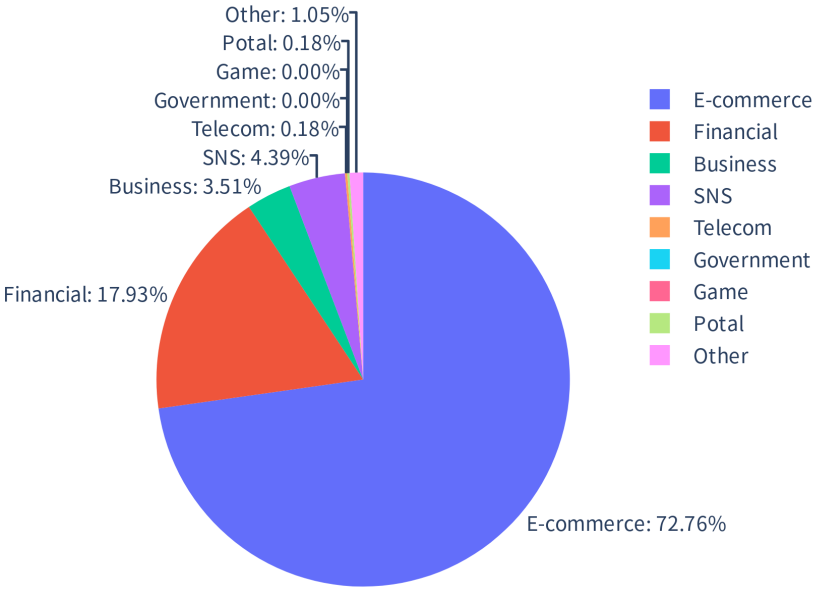

Figure 1.9 Percentage of the Number of Phishing Sites for Overseas Brands by Industry

1.2 Incident Trends

1.2.1 Trends in Phishing Sites

The number of phishing sites reported this quarter was 12,397, a 37% increase from the previous quarter's 9,063. This was also a 159% increase compared to the same period last year (4,780).

This quarter, the number of phishing sites impersonating overseas brands was 569, a 95% increase from the previous quarter's 292. The number of phishing sites impersonating domestic brands was 10,532, a 46% increase from the previous quarter's 7,235. 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 the phishing sites reported to JPCERT/CC, 72.76% of the reports related to overseas brands impersonated e-commerce sites, and 78.50% 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.

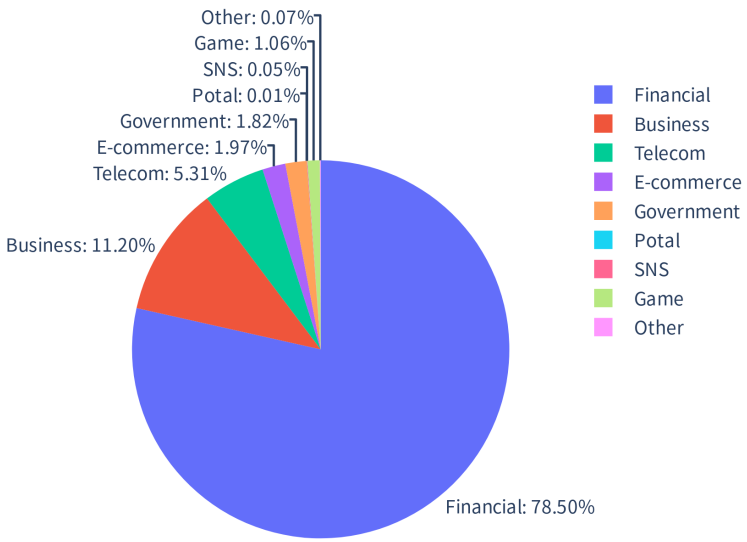

Figure 1.10 Percentage of the Number of Phishing Sites for Domestic Brands by Industry

financial sites, the largest shares in each.

For overseas brands, many phishing sites impersonated Amazon and Apple ID. For domestic brands, many reports concerned phishing sites of securities companies such as Monex, Inc. and SBI Securities. Also, many were still reported for credit card companies such as JCB, Sumitomo Mitsui Card, Saison Card, and UC Card. In addition, this quarter we also began receiving reports of phishing sites impersonating the websites of game-related companies such as PlayStation Store and Nintendo's online services. Of the sites for which we coordinated takedown of phishing sites, 99% were overseas and 1% were domestic.

1.2.2 Trends in Website Defacement

The number of website defacements reported this quarter was 105. This was a 67% decrease from the previous quarter's 319.

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

- Case 1: A form for stealing personal information was placed on a legitimate website (abuse of the Telegram API)
- Case 2: Code that displays a Cloudflare verification screen was placed on a legitimate website

In Case 1, a form (Figure 1.11) that displays a fake login screen to users accessing a legitimate website and prompts them to enter personal information had been installed. Malicious JavaScript was embedded in the form, and when the input field lost focus, the entered content was sent to the attacker via the Telegram API.

In Case 2, malicious code that displays a checkbox disguised as a Cloudflare verification screen (Cloudflare Turnstile) had been installed on a legitimate website. When the user clicks the checkbox,

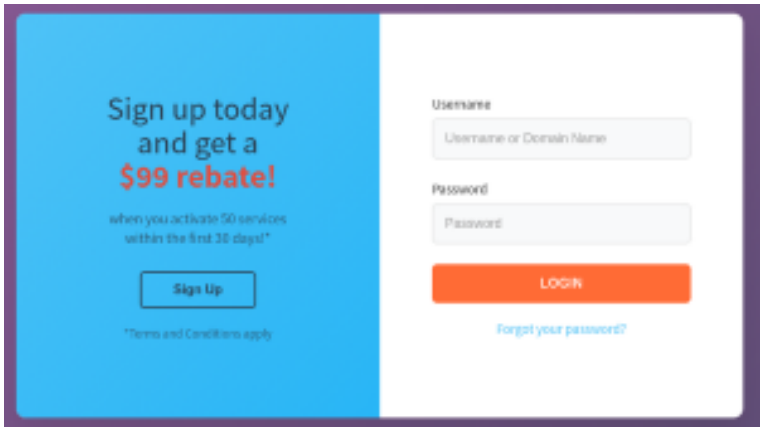

Figure 1.11 Fake Login Form

Figure 1.12 Fake Cloudflare Verification Checkbox

a message (Figure 1.12) appears prompting them to open the Run dialog with Windows key + R, paste with Ctrl + V, and then press Enter. If the user follows this message, a command that the script on the defaced web page had prewritten to the clipboard will be executed. The command copied to the clipboard executed msiexec and downloaded and ran malicious code from an external source. This method of inducing users to perform actions that execute malicious code is called ClickFix.

1.2.3 Trends in Targeted Attacks

The number of incidents classified as targeted attacks was 3.

1.2.3.1 AiTM Attacks Aiming for Microsoft Credentials

This quarter, JPCERT/CC received reports of targeted attack emails aiming for Microsoft credentials. Clicking a link in the email body displayed a page imitating OneDrive, and clicking a file

Table 1.4 Top 10 Ports by Number of Scans

Port	Oct	Nov	Dec	Total
23/tcp	79	60	41	180
22/tcp	70	38	20	128
80/tcp	33	29	16	78
25/tcp	16	14	6	36
143/tcp	6	11	2	19
443/tcp	0	11	0	11
21/tcp	5	0	0	5
85/tcp	3	0	0	3
8080/tcp	0	0	3	3
5001/tcp	1	0	1	2

shown on that page generated a fake Microsoft login pop-up. The credentials entered there were stolen by the attacker's reverse proxy.

1.2.4 Trends in Other Incidents

The number of malware sites reported this quarter was 44. This was a 38% increase from 32 in the previous quarter.

The number of scans reported this quarter was 469. This was a 3% increase from 452 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), SSH (22/TCP), HTTP (80/TCP), and SMTP (25/TCP).

The number of incidents classified as Other was 513. This was a 1% increase from 508 in the previous quarter.

1.3 Incident Response Cases

This section introduces cases handled this quarter.

1.3.1 Notifications to Domestic Organizations Infected with Rhadamanthys Identified Through Operation Endgame

In relation to Operation Endgame 3.0, JPCERT/CC received information from an external organization about hosts in Japan suspected of being infected with Rhadamanthys.

- Operation Endgame
  https://www.operation-endgame.com/

Operation Endgame is an international operation conducted through cooperation among law enforcement agencies from multiple countries, led by Europol. In Phase 3, authorities successfully seized infrastructure for multiple malware families, including Rhadamanthys, leading to the identification of many victim organizations. In response, JPCERT/CC requested the organizations managing the relevant hosts to identify infected hosts and implement remediation if infection was confirmed. We also provided advice as needed to organizations that responded and supported containment.

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 "Badsecrets" Issue Used in Web Frameworks

On October 29, 2025, JPCERT/CC published a CyberNewsFlash titled "On the Risk of Website Defacement in Web Applications Configured with Known or Weak Secrets" [*1]. When building web applications using web frameworks, if weak secrets that can be guessed or default/known secrets

[*1] "On the Risk of Website Defacement in Web Applications Configured with Known or Weak Secrets." JPCERT/CC. https://www.jpcert.or.jp/newsflash/2025102901.html, (2025-10-29)

included in sample code on the Internet are left in place in production, signature and encryption processes may be spoofed depending on the environment and conditions, potentially leading to arbitrary code execution. We therefore provided related information on responses and investigation. Issues of this kind had been pointed out by multiple organizations for about a decade. In 2023, Black Lantern Security, an overseas security company, released[*2] a tool that performs a cross-cutting check of web applications built with web frameworks affected by this issue. In the detection results from this tool shared with JPCERT/CC by the Shadowserver Foundation in September 2025 [*3], approximately 2,500 domestic hosts were included. In October of the same year, Elastic provided information on domestic hosts suspected of being infected with the TOLLBOOTH backdoor due to exploitation of this issue [*4]. In response, when we individually notified the organizations managing the hosts suspected of infection, traces of TOLLBOOTH infection were actually confirmed, and we determined that it was necessary to alert organizations in Japan that may have been potentially compromised. Therefore, we prioritized notifications from several perspectives, such as the ease of exploitation by framework, whether arbitrary code execution was possible, and the severity of potential damage, and provided information to prompt confirmation of the situation and necessary actions to reduce potential risk to the organizations using about 400 domestically hosted systems detected as being publicly exposed in a vulnerable state.

2.1.2 Vulnerability Due to Insufficient Source Verification of Communication Channels in LANSCOPE Endpoint Manager On-premises (CVE-2025-61932)

On October 20, 2025, MOTEX published an advisory [*5] regarding a vulnerability due to insufficient source verification of communication channels in LANSCOPE Endpoint Manager On-premises (CVE-2025-61932). This vulnerability was reported by the product developer as a vendor's own product report, and it was published based on the Information Security Early Warning Partnership Guideline. For details of the coordination on this case, please see 4.1.2.1.

JPCERT/CC determined that there was a possibility that attacks exploiting this vulnerability were taking place under the surface and, in coordination with the developer, published a CyberNews-Flash on the same day [*6]. We introduced information on usage cases considered to have increased likelihood of being attacked and on attack activities suggesting possible exploitation, and called on product users to implement countermeasures and conduct investigations.

[*2] "Introducing Badsecrets." Black Lantern Security. https://blog.blacklanternsecurity.com/p/introducing-badsecrets, (2023-03-20)

[*3] "HIGH: Badsecrets Report." The Shadowserver Foundation. https://www.shadowserver.org/what-we-do/network-reporting/badsecrets-report/, (2025-09-08)

[*4] "TOLLBOOTH: What's yours, IIS mine." Elastic. https://www.elastic.co/security-labs/tollbooth, (2025-10-22)

[*5] "Important Notice: Remote Code Execution Vulnerability in LANSCOPE Endpoint Manager On-premises (CVE-2025-61932)." MOTEX Inc. https://www.motex.co.jp/news/notice/2025/release251020/, (2025-10-20)

[*6] "About the Vulnerability in LANSCOPE Endpoint Manager On-Premises Edition Due to Insufficient Verification of the Source of the Communication Channel (CVE-2025-61932)." JPCERT/CC. https://www.jpcert.or.jp/newsflash/2025102001.html, (2025-10-20)

2.1.3 Unauthenticated RCE Vulnerability in WSUS (CVE-2025-59287)

On October 14, 2025 (local time), Microsoft provided a patch[*7] in its regular updates for a vulnerability in Windows Server Update Services (WSUS) involving deserialization of untrusted data (CVE-2025-59287). This vulnerability allows an attacker to execute arbitrary code by sending crafted HTTP requests to the ports used by WSUS (8530, 8531). On October 22, 2025 (local time), HawkTrace published a detailed explanation and PoC regarding this vulnerability[*8], but on October 23, 2025 (local time), Microsoft released an emergency update because the previous fix was insufficient.

Multiple security companies published information[*9][*10] stating that they observed attacks exploiting this vulnerability on or after October 24, 2025 (local time). Furthermore, on October 27, 2025, information on approximately 10 domestic hosts running WSUS was provided by an overseas organization. In light of this situation, JPCERT/CC determined that although attacks were observed, they were limited in scope, and began individual notifications to the relevant hosts on October 28, 2025. Subsequently, after receiving information from notified organizations that "the ports were opened to provide Windows Update to remote workers and business travelers," JPCERT/CC continued to investigate hosts that could be affected by this vulnerability and ultimately issued individual notifications to approximately 60 hosts, providing product users with information on the vulnerability exploitation confirmed by JPCERT/CC and on compromise investigations, and urging the implementation of countermeasures and investigations.

2.1.4 Path Traversal Vulnerability in FortiWeb (CVE-2025-64446)

On November 13, 2025 (local time), watchTowr Labs published a PoC[*11] for a path traversal vulnerability (no CVE assigned as of November 13, 2025) in Fortinet's FortiWeb. If exploited, an attacker who accesses the management console could execute arbitrary commands with administrator privileges, potentially causing severe impact. Earlier, on October 6, 2025 (local time), Defused had announced[*12] that it observed suspicious attack traffic related to Fortinet products, and following watchTowr's PoC publication, it became clear that this attack was highly likely exploiting this

[*7] "Remote Code Execution Vulnerability in Windows Server Update Services (WSUS)." Microsoft Japan Co., Ltd. https://msrc.microsoft.com/update-guide/ja-jp/vulnerability/CVE-2025-59287, (2025-10-14)

[*8] "CVE-2025-59287 WSUS Unauthenticated RCE." HawkTrace Security. https://hawktrace.com/blog/CVE-2025-59287-UNAUTH, (2025-10-22)

[*9] "Exploitation of Windows Server Update Services Remote Code Execution Vulnerability (CVE-2025-59287)." Huntress. https://www.huntress.com/blog/exploitation-of-windows-server-update-services-remote-code-execution-vulnerability, (2025-10-24)

[*10] "Windows Server Update Services (WSUS) vulnerability abused to harvest sensitive data." Sophos. https://news.sophos.com/en-us/2025/10/29/windows-server-update-services-wsus-vulnerability-abused-to-harvest-sensitive-data/, (2025-10-29)

[*11] "When The Impersonation Function Gets Used To Impersonate Users (Fortinet FortiWeb Auth. Bypass CVE-2025-64446)." watchTowr. https://labs.watchtowr.com/when-the-impersonation-function-gets-used-to-impersonate-users-fortinet-fortiweb-auth-bypass/, (2025-11-14)

[*12] "Unknown Fortinet exploit (possibly a CVE-2022-40684 variant)". "X - Defused@DefusedCyber". https://x.com/DefusedCyber/status/1975242250373517373, (2025-10-06)

vulnerability. In addition, on November 13, 2025 (local time), Rapid7 published the results of its PoC verification[*13], confirming that while the latest FortiWeb version (8.0.2) was protected, older versions such as 8.0.1 were vulnerable to exploitation.

Although the publication of the PoC raised concerns about the spread of exploitation, JPCERT/CC's investigation of domestic usage found that only about a dozen hosts were using FortiWeb, and that few hosts were affected. Therefore, rather than issuing a broad Security Alert, and given that exploitation had already been observed, we sent individual notifications to the relevant hosts on November 14, 2025. Subsequently, on the same day (November 14, 2025, local time), after Fortinet published an advisory[*14] regarding this vulnerability (CVE-2025-64446), JPCERT/CC conducted PoC verification using FortiWeb, organized the characteristics of logs observed during exploitation, added the advisory information and investigation points, and notified the target organizations again.

2.1.5 Vulnerability in ArrayAG's DesktopDirect Function

On December 3, 2025, JPCERT/CC published a Security Alert regarding a command injection vulnerability in the Array AG series by Array Networks[*15]. The company had released a version addressing this vulnerability in May 2025[*16], but JPCERT/CC had confirmed that attacks exploiting the vulnerability had occurred domestically since August 2025, including the installation of a web shell on the affected product. Although it was assumed that information about this vulnerability had already been notified to users via the developer and resellers, given the ongoing attacks in Japan, we were concerned that there might be other users who were unaware of the vulnerability information and had not confirmed damage or implemented countermeasures. Therefore, in coordination with the developer, we issued the Security Alert. At the time of publication, no information about this vulnerability had been made public, but we confirmed details such as affected targets and countermeasures with the developer, and we also shared information on the attacks that JPCERT/CC had confirmed to urge product users to implement countermeasures and conduct investigations.

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).

[*13] "CVE-2025-64446: Critical Vulnerability in Fortinet FortiWeb Exploited in the Wild". Rapid7. https://www.rapid7.com/blog/post/etr-critical-vulnerability-in-fortinet-fortiweb-exploited-in-the-wild/, (2025-11-13)

[*14] "Path confusion vulnerability in GUI". Fortinet. https://fortiguard.fortinet.com/psirt/FG-IR-25-910, (2025-11-14)

[*15] "Security Alert Regarding a Command Injection Vulnerability in the Array Networks Array AG Series". JPCERT/CC. https://www.jpcert.or.jp/at/2025/at250024.html, (2025-12-03)

[*16] "Array OS release 9.4.5.9 for the Array AG 1000 series is now available for download.". "X - Array Support@ArraySupport". https://x.com/ArraySupport/status/1921373397533032590, (2025-05-11)

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 6 items and updated 2 items.

- 2025-10-01 Security Alert Regarding Multiple Vulnerabilities in Cisco ASA and FTD (CVE-2025-20333, CVE-2025-20362) (Update)
- 2025-10-15 Security Alert Regarding the October 2025 Microsoft Security Updates (Publication)
- 2025-11-12 Security Alert Regarding the November 2025 Microsoft Security Updates (Publication)
- 2025-12-03 Security Alert Regarding a Command Injection Vulnerability in the Array Networks Array AG Series (Publication)
- 2025-12-05 Security Alert Regarding a Command Injection Vulnerability in the Array Networks Array AG Series (Update)
- 2025-12-10 Security Alert Regarding Vulnerabilities in Adobe Acrobat and Reader (APSB25-119) (Publication)
- 2025-12-10 Security Alert Regarding the December 2025 Microsoft Security Updates (Publication)
- 2025-12-22 Security Alert Regarding an Out-of-bounds Write Vulnerability in iked of WatchGuard Firebox (CVE-2025-14733) (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 5 items and updated 2 items.

- 2025-10-20 Vulnerability of Insufficient Source Verification in a Communication Channel in LANSCOPE Endpoint Manager On-Premises (CVE-2025-61932)

- 2025-10-21 On the Out-of-bounds Write Vulnerability in iked of WatchGuard Firewall "Firebox" (CVE-2025-9242)
- 2025-10-22 Vulnerability of Insufficient Source Verification in a Communication Channel in LANSCOPE Endpoint Manager On-Premises (CVE-2025-61932) (Update)
- 2025-10-24 Multiple Vulnerabilities in ISC BIND 9 (October 2025)
- 2025-10-29 Risk of Website Defacement in Web Applications Configured with Known or Weak Secrets
- 2025-12-05 Vulnerability in React Server Components (CVE-2025-55182)
- 2025-12-10 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 13 issues and provided a total of 99 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, 60 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 78 items. We provided information to organizations that manage hosts affected by issues such as the Badsecrets issue used in web frameworks, the unauthenticated RCE vulnerability in WSUS (CVE-2025-59287), and the path traversal vulnerability in FortiWeb (CVE-2025-64446).

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 sent to 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. 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 each organization 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 Threat Monitoring Report and the blog "TSUBAME Report Overflow," which introduce observation

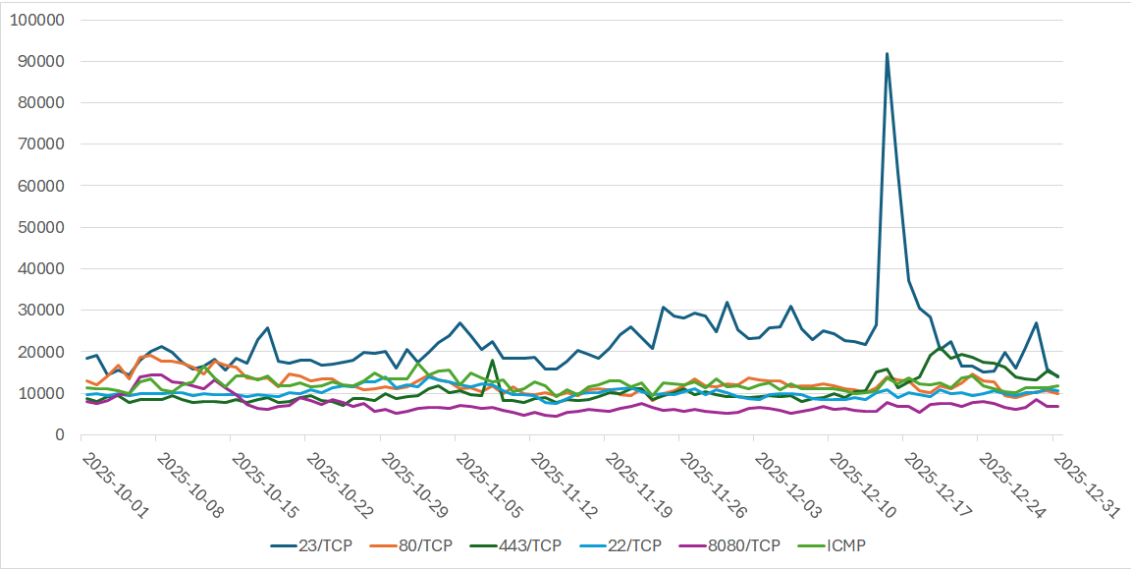

Figure 3.1 Packet Counts for Top-Ranked Destination Ports 1–5 Observed by TSUBAME (October 1, 2025–December 31, 2025)

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 following 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 temporary increases around November 19, 2025 and December 15, 2025. 80/TCP ranked second. 443/TCP ranked third and 22/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.

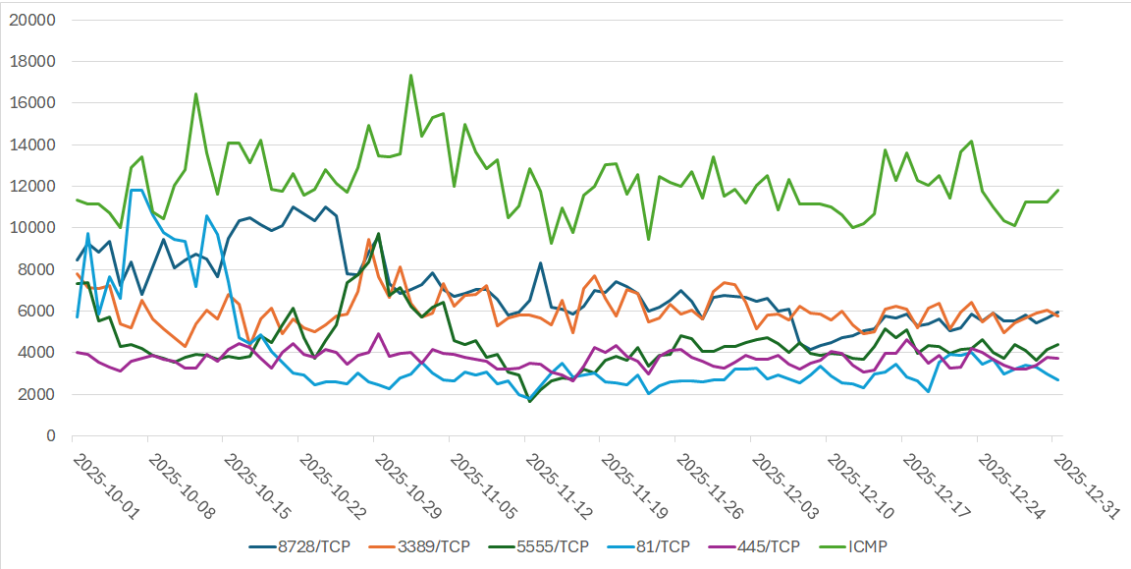

Figure 3.2 Packet Counts for Top-Ranked Destination Ports 6–10 Observed by TSUBAME (October 1, 2025–December 31, 2025)

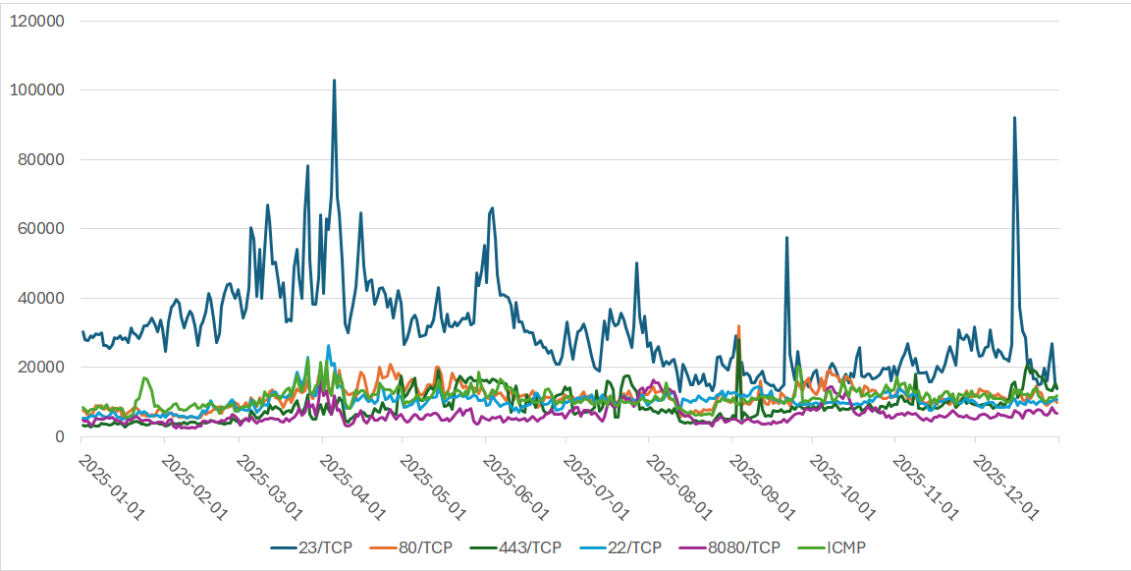

Figure 3.3 Packet Counts for Top-Ranked Destination Ports 1–5 Observed by TSUBAME (January 1, 2025–December 31, 2025)

Trends over the past year (January 1, 2025–December 31, 2025) 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. This quarter, we confirmed communications related to a vulnerability in React Server Components (CVE-2025-55182).

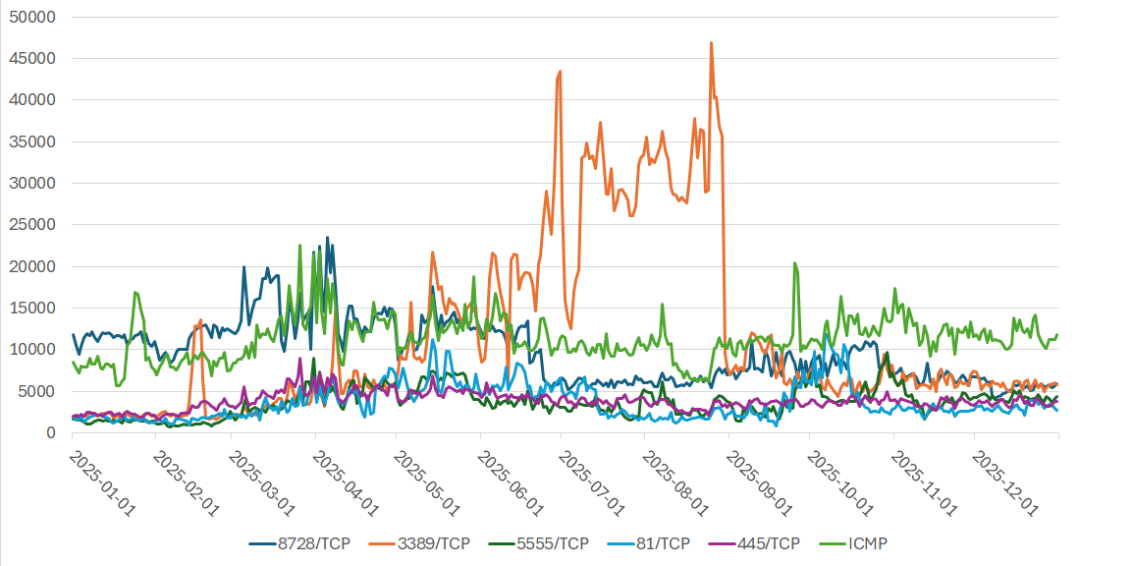

Figure 3.4 Packet Counts for Top-Ranked Destination Ports 6–10 Observed by TSUBAME (January 1, 2025–December 31, 2025)

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, 142 vulnerability advisories were published on JVN, bringing the cumulative total to 6,139; 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: 39
- Items related to vulnerability information through international or independent coordination: 103
- Items related to technical information associated with vulnerability information: 0

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

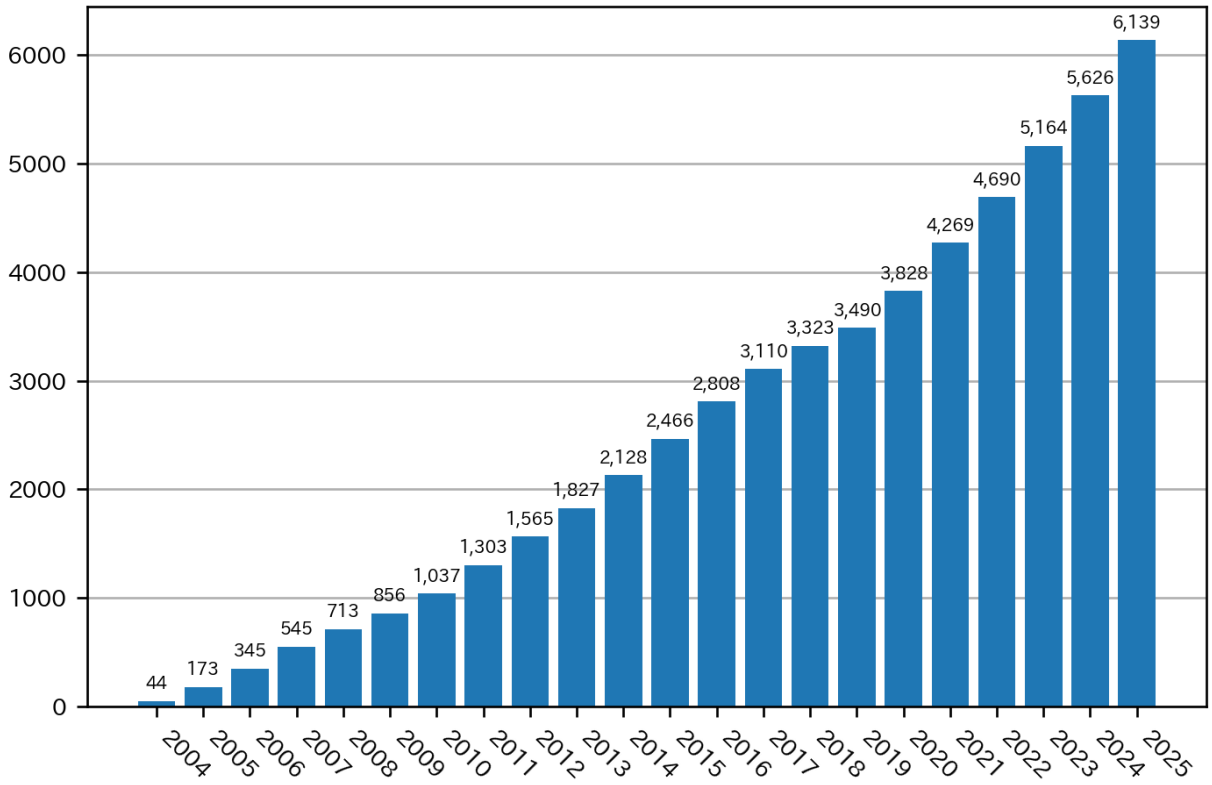

Figure 4.1 Cumulative Number of JVN Publications

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#86318557
  Improper Source Verification in Communication Channel in LANSCOPE Endpoint Manager On-premises
  https://jvn.jp/jp/JVN86318557/

This is a vulnerability in the IT asset management tool "LANSCOPE Endpoint Manager On-premises" provided by MOTEX. This vulnerability was reported as a self-report by the product developer. During coordination, it was found that suspicious packets potentially attempting to exploit the vulnerability in customer environments had been observed. Although JPCERT/CC did not obtain information to conclusively determine exploitation activities, we assessed that attacks might be occurring covertly. IT asset management tools are mainly used in organizations such as companies, and exploitation of a vulnerability could affect the organization's operations themselves.

When publishing the JVN advisory, we marked the title as “Urgent” and stated in the details, “According to the developer, there have been confirmed cases of receiving malicious packets from external sources in customer environments,” urging organizations to respond promptly. After publishing the advisory, we also issued a CyberNewsFlash as an alert related to this matter, indicating product operating environments considered to be at high risk of attack to call for further caution. For details on the publication of the alert related to this matter, please refer to 2.1.2.

4.1.2.2 Notable Vulnerabilities Handled via International or Independent Coordination

There were no noteworthy vulnerabilities this quarter.

4.1.2.3 Other Noteworthy Items Related to Vulnerability Coordination

As an example of collaboration between security researchers and coordination bodies in Coordinated Vulnerability Disclosure (CVD), we introduce vulnerabilities in Fuji Electric’s drawing software V-SFT that were published this quarter.

- JVNVU#90008453
  Multiple Vulnerabilities in Fuji Electric V-SFT
  https://jvn.jp/vu/JVNVU90008453/

Fuji Electric’s graphics creation software V-SFT is used for designing applications for the company’s programmable displays, and this advisory points out nine vulnerabilities. In addition, three other advisories (JVNVU#97228144, JVNVU#94011267, JVNVU#93984110) were published on JVN this fiscal year. Three of the four advisories in total are related to 22 vulnerabilities reported by security researcher Michael Heinzl. He has reported many vulnerabilities in industrial/control systems and devices, and JPCERT/CC presented him with the Best Reporter Award in 2022 (https://www.jpcert.or.jp/award/best-reporter-award/2022.html). Since then, he has continued to diligently analyze vulnerabilities contained in Japanese products and has practiced responsible disclosure. Besides him, there are many people who discover vulnerabilities in products within their areas of expertise—such as smartphone apps, network equipment, and product installers—and report them on an ongoing basis. JPCERT/CC’s CVD activities are made possible through the cooperation of reporters and developers who are proactive in improving the security quality of the products they provide, but depending on the situation, their interests may conflict. Reporters who explore vulnerabilities as researchers may wish to publish the detected vulnerabilities in time with academic conference schedules as research findings or supporting evidence. On the other hand, developers prefer publication after securing the time needed for investigation and for creating and providing patches. If coordination fails and vulnerability information is disclosed before patches are provided, product users may be exposed to attack risk. To prevent such situations, JPCERT/CC strives to facilitate smooth information sharing so that reporters are properly recognized for their capabilities and developers can protect product users, enabling mutual understanding of each other’s situations. Publication of a JVN advisory like this case is the result of CVD activities by all parties involved.

By steadily carrying out such coordination activities, building trust with more stakeholders, and maintaining cooperative relationships, we aim to promote CVD.

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 87 vulnerabilities.

For details about 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

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 1,325, as shown in Figure 4.2. This quarter, we reviewed registrants' activity status and deleted registrations of product developers from whom vulnerability handling could not be expected due to business closure or termination of activities. The above number of registrations reflects the decrease due to these deletions. For details on registration, please refer to the following web page.

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

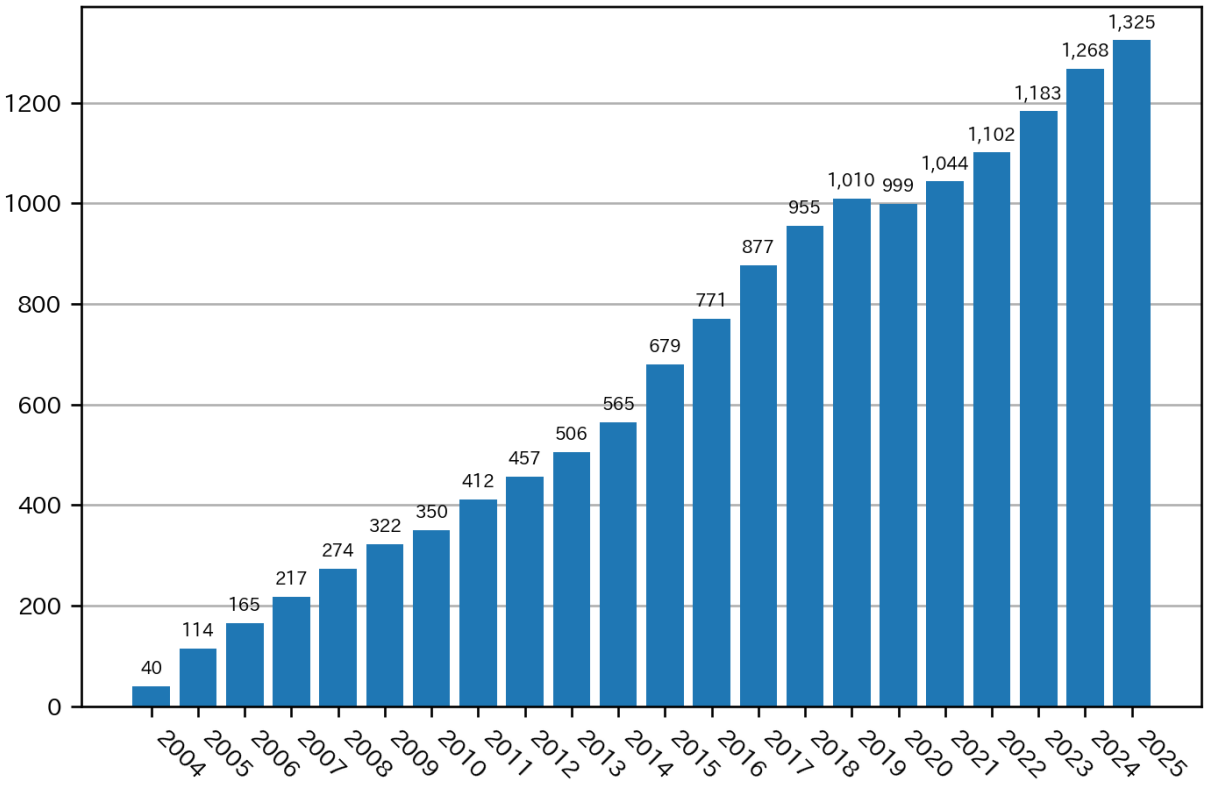

Figure 4.2 Number of Registered Product Developers

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 Japan Foreign Trade Council ISAC

We participated in the Practical Working Group held on November 21, 2025, and gave a presentation titled "Response to Incidents Exploiting Vulnerabilities: Attacks Exploiting Multiple Vulnerabilities Such as Ivanti Connect Secure."

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

We participated in the Security Research Joint Working Group regularly held by SICE (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.

5.1.3 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 82nd CEPTOAR Council Steering Committee held on December 8, 2025, we shared information about the status of attack activities that exploit vulnerabilities in Windows Server Update Services (WSUS).

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, 13 new organizations registered as CISTA users.

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

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

As of the end of this quarter, 36 organizations were participating.

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.

6.1.1 Participation in the 2025 FIRST & AfricaCERT Symposium: Africa and Arab Regions

From December 2 to December 5, 2025, a symposium for the Africa and Arab regions co-hosted by FIRST and AfricaCERT was held in Mauritius. JPCERT/CC participated in this event and exchanged views with CSIRT personnel from African countries. In addition, on December 4, 2025, Koichiro Komiyama, Director of the Global Coordination Division, delivered a presentation titled "Sharing our CVD Journey: Insights and Lessons," sharing JPCERT/CC's insights and challenges in vulnerability handling. For details of the event, please refer to the web page below.

- 2025 FIRST & AfricaCERT Symposium: Africa and Arab Regions
  https://www.first.org/events/symposium/africa-arab-regions2025/

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 teleconferences on October 9 and November 18, 2025, 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.

6.2.1.2 Participation in the APCERT Annual General Meeting and Conference 2025

From November 25 to November 28, 2025, APCERT's Annual General Meeting and Conference was held in Sydney, Australia. Under the theme "Cyber Horizons: Strengthening Regional Resilience - Together," approximately 100 participants attended, including APCERT member and partner organizations and representatives of Australia's cybersecurity community. The Annual General Meeting was attended by 21 of the 34 Operational Members, which are APCERT's primary members, including JPCERT/CC. In the election to fill three Steering Committee seats whose terms had expired, CyberSecurity Malaysia (Malaysia) and Sri LankaCERT|CC (Sri Lanka) were re-elected along with JPCERT/CC. JPCERT/CC was also re-elected as the Secretariat. In the election for Chair and Deputy Chair teams, ACSC (Australia) was elected as the Chair team and KrCERT/CC (Korea) as the Deputy Chair team. JPCERT/CC will continue to lead various activities as the APCERT Secretariat and a member of the Steering Committee. At the Open Conference held on November 28, 2025, Yukako Uchida, a manager in the Global Coordination Division and a FIRST Board member, gave a presentation on FIRST's global community activities.

6.2.2 FIRST (Forum of Incident Response and Security Teams)

Since joining in 1998, JPCERT/CC has actively participated in FIRST activities, and since June 2021, Yukako Uchida of the Global Coordination Division has served on the Board. This quarter, we participated in the monthly online Board meetings. 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.

6.3.1 Visit to CERT-PH in the Philippines

On November 19, 2025, we visited the office of CERT-PH in the Philippines. We interviewed them about their activities and exchanged views on future collaboration.

6.3.2 Visit from KISA in Korea

On November 26, 2025, the Korea Internet & Security Agency (KISA) visited JPCERT/CC's office. We interviewed them about their activities and exchanged views on future collaboration.

6.3.3 Visit from CSA in Singapore

On December 3, 2025, the Cyber Security Agency (CSA) in Singapore visited JPCERT/CC's office. We interviewed them about their activities and exchanged views on future collaboration.

6.3.4 Visit to CERT-MU in Mauritius

On December 5, 2025, we visited the office of CERT-MU in Mauritius. We toured the organization's Security Operations Center, interviewed them about their activities, and exchanged views on future collaboration.

6.3.5 Visits to Public CSIRT/CC, MNCERT/CC, and the National CSIRT in Mongolia

On December 12, 2025, we visited CSIRT-related organizations in Mongolia (Public CSIRT/CC, MNCERT/CC, and the National CSIRT). We interviewed them about their activities and exchanged views on future collaboration.

6.4 Participation in Other International Conferences

6.4.1 Panel Participation at Enhancing Cyber Resilience: Approach, Responses, and Practical Actions

On November 25, 2025, Koichiro Komiyama, Director of the Global Coordination Division, participated in the conference Enhancing Cyber Resilience: Approach, Responses, and Practical Actions hosted by the ADR Institute for Strategic and International Studies. He joined a panel session on cyber resilience and spoke about the role of CERTs.

- Stratbase Pilipinas Conference 2025: Enhancing Cyber Resilience: Approach, Responses, and Practical Actions
  https://adrinstitute.org/2025/11/20/stratbase-pilipinas-conference-2025-enhancing-cyber-resilience-approach-responses-and-practical-actions/

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 in WG3, substantive revision work began for both ISO/IEC 29147 (Vulnerability disclosure) and 30111 (Vulnerability handling processes), including discussions on updates and the drafting of Working Drafts.

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

JPCERT/CC has established cooperative relationships with overseas coordination organizations that coordinate vulnerability information in each region, such as CISA and CERT/CC in the United States, and has collaborated with them to facilitate smooth international coordination and information sharing of vulnerability information. In addition, we participated in international community activities related to vulnerabilities, including FIRST, and worked on building a foundation for collaboration.

6.6.1 Presentation at a Workshop During the Japan-U.S.-EU Industrial Control System Cybersecurity Week for the Indo-Pacific Region

From November 18 to November 21, 2025, the Ministry of Economy, Trade and Industry and the Industrial Cyber Security Center of Excellence (ICSCoE), in collaboration with the U.S. and EU governments, held the Japan-U.S.-EU Industrial Control System Cybersecurity Week for the Indo-Pacific Region.

Practitioners from industry and government agencies in the Indo-Pacific region participated in the event, which featured workshops using industry-specific scenarios and hands-on exercises against cyberattacks in the industrial control field. JPCERT/CC delivered a workshop on vulnerability management and SBOM, presented on the basics of vulnerability coordination and international challenges, and led discussions with participants. For details of the event, please refer to the following web page.

- The Ministry of Economy, Trade and Industry Held the Japan-U.S.-EU Industrial Control System Cybersecurity Week for the Indo-Pacific Region
  https://www.meti.go.jp/press/2025/11/20251125001/20251125001.html

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 it has received 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

The number of phishing reports has continued to remain at a high level. Although the figure for this quarter has not been finalized, Figure 7.1 shows the trend in the number of phishing reports over the past year.

By breakdown of reports, those impersonating "Amazon" were the most numerous, accounting for about 13.0% of the total. This was followed by reports of phishing impersonating "Apple," accounting for about 6.1% of the total.

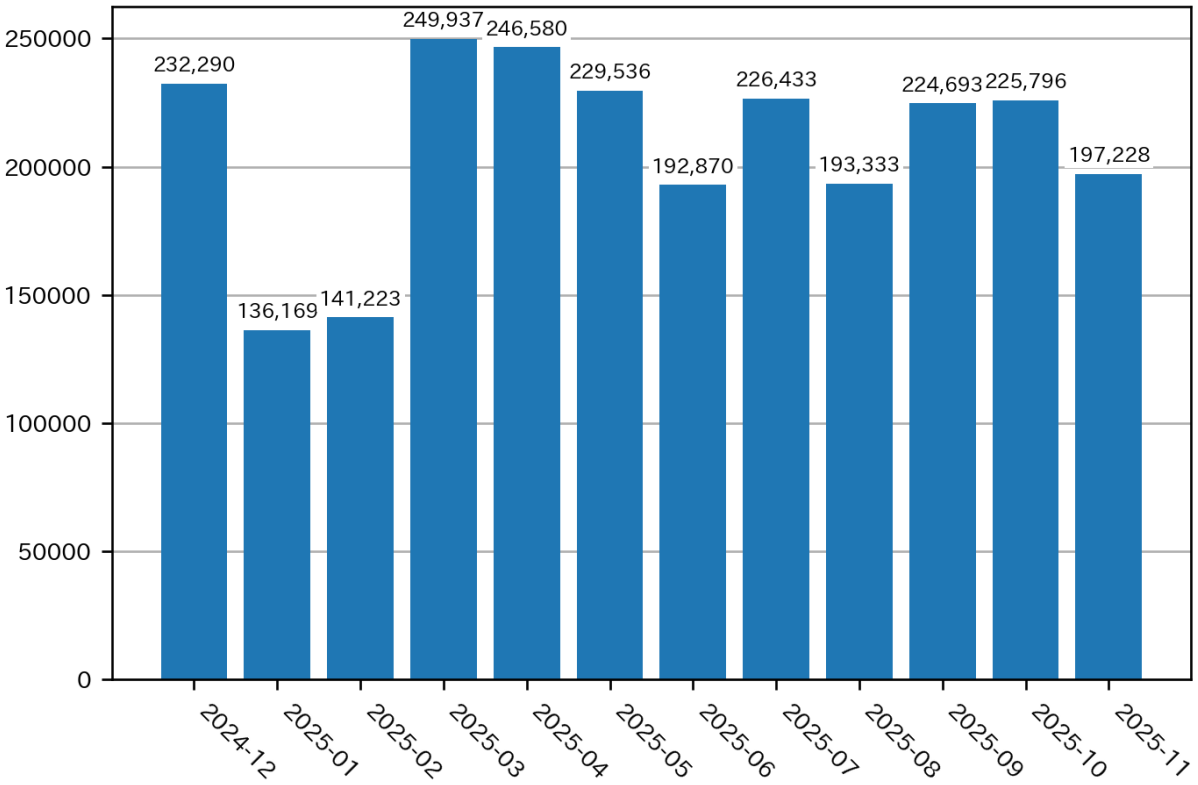

Figure 7.1 Number of Phishing Reports

7.1.2 Information Gathering and Distribution

7.1.2.1 Distribution of Information on Phishing Trends, etc.

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

- Phishing impersonating Japan Post
- Phishing impersonating the Official Lottery Website
- Phishing impersonating OpenAI (ChatGPT)
- Phishing impersonating Lawson Ticket
- Phishing impersonating Mizuho Securities

This quarter, in addition to an increase in phishing impersonating brands that had been targeted in the past, phishing impersonating delivery and transportation services occurred, apparently timed to the year-end gift season and periods of heavy travel. Other cases included attempts to solicit phone numbers under the guise of a national census request and then misuse them to prompt entry of authentication codes to bypass two-factor authentication of targeted online services (Figure 7.2), as well as phishing that lured users with messages offering lottery gifts (Figure 7.3).

Figure 7.2 Example of a Phishing Site Masquerading as a National Census Request

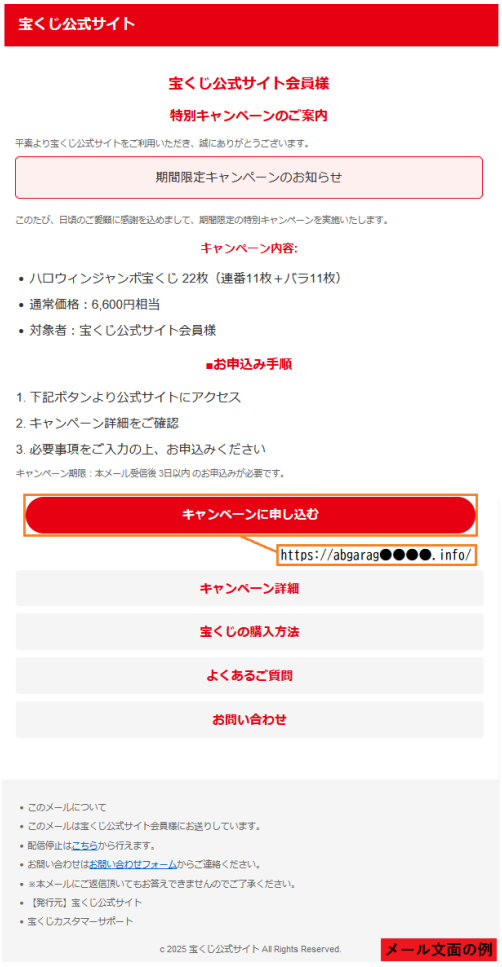

Figure 7.3 Example of a Phishing Email Impersonating the Official Lottery Website

7.1.2.2 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/
- 2025/09 Phishing Report Status
  https://www.antiphishing.jp/report/monthly/202509.html
- 2025/10 Phishing Report Status
  https://www.antiphishing.jp/report/monthly/202510.html
- 2025/11 Phishing Report Status
  https://www.antiphishing.jp/report/monthly/202511.html

7.1.2.3 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 URL information to 50 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.

- 132nd Steering Committee (JPCERT/CC Conference Room + Online)
  Date/Time: October 23, 2025, 16:00–18:00
- 133rd Steering Committee (JPCERT/CC Conference Room + Online)
  Date/Time: November 27, 2025, 16:00–18:00
- 134th Steering Committee (JPCERT/CC Conference Room + Online)
  Date/Time: December 25, 2025, 16:00–18:00

7.2.2 Support for Holding Working Group Meetings, etc.

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

- Academic Research Working Group Meeting
  Date/Time: Every Tuesday from October 2025 to December 2025, 9:00–9:30 (Online)
- 2nd Technical and Institutional Study Working Group
  Date/Time: October 8, 2025, 16:30–18:00 (JPCERT/CC Conference Room + Online)
- 3rd Technical and Institutional Study Working Group
  Date/Time: November 6, 2025, 15:30–18:00 (JPCERT/CC Conference Room + Online)
- 20th Anniversary Seminar of the Council of Anti-Phishing Japan
  Date/Time: November 14, 2025, 13:00–19:30 (Akasaka Intercity Conference the Air + Online)
- Certificate Promotion Working Group Meeting
  Date/Time: December 2, 2025, 16:00–17:30 (JPCERT/CC Conference Room + Online)

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.

- Software Quality Improvement Seminar
  Title: Research Trends in Vulnerabilities of Embedded and Control Systems and Basic Concepts of Secure Development
  Presenter: Ikuya Fukumoto (Vulnerability Analyst, Early Warning Group)
  Organizer: TechMatrix
  Presentation date: October 16, 2025
- Internet Week 2025
  Title: The Current State of Phishing and the Latest Countermeasures (2025 Edition)
  Presenter: Nobuyo Hiratsuka (Information Security Analyst, Domestic Coordination Group)
  Organizer: Japan Network Information Center
  Presentation date: November 19, 2025
- Internet Week 2025
  Title: What Does "Cybersecurity" Aim For? Measures and Thinking Required of Defenders
  Presenter: Hayato Sasaki (General Manager of Strategy and Early Warning Group Manager, Threat Analyst)
  Organizer: Japan Network Information Center
  Presentation date: November 20, 2025
- Internet Week 2025
  Title: Considering Spoofed Emails and DMARC: Delivery Status of Phishing Emails (2025

Edition)
Presenter: Nobuyo Hiratsuka (Information Security Analyst, Domestic Coordination Group)
Organizer: Japan Network Information Center
Presentation date: November 20, 2025

- Internet Week 2025
  Title: Edge Devices Under Constant Attack: Cyberattacks from JPCERT/CC's Perspective
  Presenter: Tatsuya Kuge (Threat Information Analyst, Early Warning Group)
  Organizer: Japan Network Information Center
  Presentation date: November 25, 2025
- Security Talent Development Program
  Title: Toward an Agile CSIRT
  Presenter: Nobukatsu Toudou (Threat Information Analyst, Early Warning Group)
  Organizer: Kansai Institute of Information Systems
  Presentation date: December 4, 2025
- Cybersecurity Seminar
  Title: Introduction to Incident Response: Key Points to Minimize Secondary Damage
  Presenter: Hayato Sasaki (General Manager of Strategy and Early Warning Group Manager, Threat Analyst)
  Organizer: JTB Business Innovators
  Presentation date: December 11, 2025
- Infoblox Exchange Tokyo 2025
  Title: Trends in DNS Abuse from Case Studies and Their Impact on Japan
  Presenter: Naoko Nakai (Senior Incident Coordinator, Incident Response Group)
  Organizer: Infoblox
  Presentation date: December 11, 2025
- ESET Cybersecurity Day in Tokyo
  Title: Edge Devices Under Constant Attack: Cyberattack Trends Seen from JPCERT/CC Activities
  Presenter: Mitsutaka Hori (Threat Information Analyst, Early Warning Group)
  Organizer: ESET Japan
  Presentation date: December 11, 2025
- FY2025 Civil Engineering Department Staff Training "Cybersecurity Training"
  Title: Cybersecurity Training
  Presenter: Ryusuke Shiraishi (Threat Information Analyst, Early Warning Group)
  Organizer: Miyagi Prefecture
  Presentation date: December 19, 2025

8.2 Publications

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

- Measurement Technology, November 2025 Issue
  Title: Security of Control Systems in Japan: Past and Future Outlook
  Toshio Miyachi (Expert Advisor)
  Publisher: JAPAN INDUSTRIAL PUBLISHING
  Publication date: November 5, 2025

8.3 Support and Sponsorship

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

- The 37th Annual Conference of the Japan Society of Security Management
  Organizer: Japan Society of Security Management
  Event date: October 4, 2025
- 3rd Chubu/Tokai Critical Infrastructure & Industrial Cybersecurity Conference
  Organizer: Critical Infrastructure Cybersecurity Conference Executive Committee
  Event date: October 7, 2025
- Hardening 2025 Invisible Divide
  Organizer: Hardening Project Executive Committee
  Event dates: October 8, 2025–October 10, 2025
- Information Security Workshop in Echigo-Yuzawa 2025
  Organizer: Association of Niigata Information Security; Information Security Workshop in Echigo-Yuzawa Executive Committee
  Event dates: October 10, 2025–October 11, 2025
- Security Days Fall 2025
  Organizer: NANO OPT Media
  Event dates: October 10, 2025–October 28, 2025
- 25th Anti-Spam Measures Conference
  Organizer: Internet Association Japan
  Event dates: November 4, 2025–November 5, 2025
- JAIPA Cloud Conference 2025
  Organizer: Japan Internet Providers Association, Cloud Working Group
  Event date: November 4, 2025
- Internet Week 2025
  Organizer: Japan Network Information Center
  Event dates: November 18, 2025–November 27, 2025

- Digital Forensic Community 2025 in TOKYO
  Organizer: Digital Forensic Study Group; Digital Forensic Community 2025 Executive Committee
  Event dates: December 8, 2025–December 9, 2025
- Security Management Conference 2025 Winter
  Organizer: SB Creative
  Event dates: December 10, 2025–December 11, 2025

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.

- 2025-10-24
  JPCERT/CC Internet Threat Monitoring Report [April 1, 2025 - June 30, 2025]
  https://www.jpcert.or.jp/english/doc/TSUBAMEReport2025Q1_en.pdf

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.

- 2025-10-16
  Status of Reports on Software Vulnerability-Related Information [Q3 2025 (July–September)] (Japanese)
  https://www.jpcert.or.jp/pr/2025/vulnREPORT_2025q3.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 five articles.

Japanese edition: 2 articles https://blogs.jpcert.or.jp/ja/

- 2025-10-27
  Update on Attacks by the Threat Group APT-C-60
- 2025-11-18
  YAMAGoya: A Real-time Client Monitoring Tool Using Sigma and YARA Rules

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

- 2025-10-28
  TSUBAME Report Overflow (Apr-Jun 2025)
- 2025-11-05
  Update on Attacks by Threat Group APT-C-60
- 2025-11-18
  YAMAGoya: A Real-time Client Monitoring Tool Using Sigma and YARA Rules

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/
- Providing incident information and requesting response: 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 PGP public keys: https://www.jpcert.or.jp/jpcert-pgp.html

JPCERT/CC Quarterly Report [October 1, 2025 to December 31, 2025]

- Revision History
  - January 22, 2026 First Japanese version
  - July 23, 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/