



JPCERT/CC Quarterly Report

April 1, 2026 to June 30, 2026

July 16, 2026



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.jpccert.or.jp/qr/>

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 2026 Fiscal Year” (a project commissioned by the Ministry of Economy, Trade and Industry) and “Administrative Activities for Dissemination of Incident Information and Related Matters to Enhance Cyber Response Capabilities for the 2026 Fiscal Year” (a project commissioned by the Cabinet Secretariat).

This document reports on activities from April 1, 2026 to June 30, 2026.

Note that “Chapter 4 Domestic Collaboration Activities,” “Chapter 5 International Collaboration Activities,” “Chapter 6 Council of Anti-Phishing Japan Activities,” and “Chapter 7 Public Relations Activities” include some descriptions of voluntary activities other than sponsored activities.

In October 2026, JPCERT/CC will mark its 30th anniversary. We would like to express our sincere gratitude to everyone who has supported our activities.

Contents

Introduction	2
Topics & Highlights	6
Presentation of JPCERT/CC Certificates of Appreciation for FY2026	6
Integration of the Internet Threat Monitoring Report into the Quarterly Report	6
Chapter 1 Incident Response Support and Threat Intelligence Analysis	8
1.1 Incident Response Support	8
1.1.1 Quarterly Statistical Information	8
1.1.2 Incident Trends	14
1.1.2.1 Trends in Phishing Sites	14
1.1.2.2 Trends in Website Defacement	14
1.1.2.3 Trends in Targeted Attacks	16
Targeted Attack Emails Abusing Legitimate Cloud Services	16
1.1.2.4 Trends in Other Incidents	16
1.2 Analysis and Provision of Threat Intelligence	17
1.2.1 Information Collection and Analysis	17
1.2.2 Information Provided on the Website	17
1.2.2.1 Security Alerts	17
1.2.2.2 Weekly Report	18
1.2.3 Information Provided via CISTA	19
1.2.3.1 Early Warning Information	19
1.2.3.2 Analyst Note	19
1.2.3.3 Indicator Information	19
1.2.3.4 Individually Provided Information	19
1.2.4 Response Cases	20
1.2.4.1 Authentication Bypass Vulnerability in cPanel and WHM (CVE-2026-41940)	20
1.2.4.2 Stack-Based Buffer Overflow Vulnerability in GUARDIANWALL MailSuite (CVE-2026-32661)	21
1.2.4.3 Authentication Bypass Vulnerability in Cisco Catalyst SD-WAN Controller (CVE-2026-20182)	21
Chapter 2 Observation and Analysis of Reconnaissance and Attack Activities on the Internet	23
2.1 Monitoring Using the Internet Threat Monitoring System “TSUBAME”	23
2.1.1 Utilization of TSUBAME Observation Data	23
2.1.2 TSUBAME Observation Trends	24
2.2 Honeypot Operation and Analysis	25

2.2.1	Observation of Attack Activity Targeting a Vulnerability in React Server Components (CVE-2025-55182)	26
2.2.2	Communications Targeting Vulnerabilities in LLM-Related Frameworks . . .	27
Chapter 3	Coordination and Dissemination of Vulnerability-Related Information	28
3.1	Handling Status of Vulnerability-Related Information	28
3.1.1	Handling of Vulnerability-Related Information at JPCERT/CC	28
3.1.2	Vulnerability Information and Response Status Published on Japan Vulnerability Notes (JVN)	29
3.1.2.1	Notable Vulnerabilities Reported Based on the Partnership Guideline	30
	JVN#35567473 Stack-Based Buffer Overflow Vulnerability in GUARDIAN-WALL MailSuite	30
	JVN#00263243, JVN#57877356 Handling of Vulnerabilities in Tools Provided by JPCERT/CC (EmoCheck, LogonTracer)	31
3.1.2.2	Notable Vulnerabilities Handled via International or Independent Coordination	31
3.1.2.3	Other Notable Matters Related to Vulnerability Coordination	31
	JVNVU#96777324 Updates for Intel Products (May 2026)	31
3.1.3	Handling of Unreachable Developers	32
3.1.4	Activities as a CNA and Root	32
3.2	Development of a Vulnerability Information Distribution Framework in Japan . . .	33
3.2.1	Collaboration with Product Developers in Japan	33
Chapter 4	Domestic Collaboration Activities	35
4.1	Collaboration with Industry Associations and Communities	35
4.1.1	SICE/JEITA/JEMIMA Joint Working Group on Security Research	35
4.1.2	CEPTOAR Council Steering Committee	35
4.2	Strengthening Collaboration and Establishing Information Exchange Environments with Domestic Stakeholders	36
4.2.1	Promoting Collaboration with CISTA Users	36
4.2.2	Working Group for Control System Security Personnel in the Manufacturing Industry	36
4.3	Provision of Information and Tools	36
4.3.1	Provision of Self-assessment Tools for Control System Security	36
Chapter 5	International Collaboration Activities	37
5.1	Support for Building and Operating Overseas CSIRTs	37
5.2	International CSIRT Collaboration	37
5.2.1	APCERT (Asia Pacific Computer Emergency Response Team)	37
5.2.1.1	Holding of the APCERT Steering Committee Meeting	38
5.2.2	FIRST (Forum of Incident Response and Security Teams)	38
5.2.2.1	Participation in the 38th Annual FIRST Conference	38
5.3	Visits to and from Overseas CSIRTs, etc.	38
5.4	Participation in Other International Conferences	39
5.4.1	Participation in Locked Shields	39
5.4.2	Participation in NatCSIRT 2026	39
5.5	International Standardization Activities	39

5.6	Building an International Cooperative Framework for Vulnerability Coordination and Information Sharing	40
5.6.1	Participation in CVE/FIRST VulnCon 2026 & Annual CNA Summit	40
Chapter 6	Council of Anti-Phishing Japan Activities	41
6.1	Operation of the Secretariat of the Council of Anti-Phishing Japan	41
6.1.1	Acceptance of Phishing Reports and Inquiries	41
6.1.2	Information Gathering and Distribution	42
6.1.2.1	Regular Reports	42
6.1.2.2	Provision of Phishing Site URL Information	43
6.1.2.3	Publication of Anti-Phishing Guidelines and the Phishing Report . . .	43
6.2	Activities for Member Organizations of the Council of Anti-Phishing Japan	44
6.2.1	Steering Committee Meetings	44
6.2.2	Support for Holding Working Group Meetings, etc.	44
Chapter 7	Public Relations Activities	45
7.1	Presentations	45
7.2	Support and Sponsorship	45
7.3	Published Materials	46
7.3.1	Internet Threat Monitoring Report	46
7.3.2	Status of Reports on Software Vulnerability-Related Information	46
7.3.3	Official Blog “JPCERT/CC Eyes”	47
Appendix A	Incident Categories	48

Topics & Highlights

Presentation of JPCERT/CC Certificates of Appreciation for FY2026

JPCERT/CC conducts activities to support incident response, early warning activities to prevent incidents, malware analysis, and coordination activities concerning vulnerabilities in software products and other items in order to reduce damage caused by various cyberattacks in Japan. These activities are made possible by the information and various forms of cooperation provided by many individuals and organizations. JPCERT/CC presents certificates of appreciation to those who have made significant contributions to cybersecurity efforts through such information sharing and cooperation.

This fiscal year, we presented a certificate of appreciation to OMRON PSIRT of OMRON Corporation.

OMRON PSIRT has carried out activities that serve as a model for other product developers through its advanced initiatives in product security and extensive track record in vulnerability handling. It has also contributed to JPCERT/CC's activities in a wide range of areas. For details of this fiscal year's presentation of the certificate of appreciation, please see the following web page.

- JPCERT/CC Certificates of Appreciation 2026
<https://www.jpcert.or.jp/award/appreciation-award/2026.html>

Integration of the Internet Threat Monitoring Report into the Quarterly Report

JPCERT/CC has distributed multiple observation sensors across the Internet and built and operates the Internet threat monitoring system TSUBAME. Data collected by TSUBAME is analyzed in comparison with vulnerability information, malware information, attack tool information, and other data. We have mainly provided information on TSUBAME observations and analysis results through the “JPCERT/CC Internet Threat Monitoring Report”, the “JPCERT/CC Quarterly Report”, and “TSUBAME Report Overflow” (blog articles). Of these, the “Internet Threat Monitoring Report” has been integrated into the “Quarterly Report” starting this fiscal year. This change is intended to clearly communicate the observation results and insights obtained through Internet threat monitoring while preventing content from being dispersed across multiple reports or the

content and perspectives from becoming unclear. We will continue to share insights through the “Quarterly Report” with those who have been reading the “Internet Threat Monitoring Report.” We would also appreciate feedback from those who have started reading the “Quarterly Report” as a result of this change, particularly their fresh perspectives on Internet threat monitoring and the utilization of its results.

We will continue to strive to provide effective information so that insights obtained from Internet threat monitoring can help users identify potential issues in their systems, such as inappropriate settings and unaddressed vulnerabilities, and take action to address them.

Chapter 1

Incident Response Support and Threat Intelligence Analysis

1.1 Incident Response Support

JPCERT/CC accepts reports of incidents that occur in Japan and overseas^{*1}. In this section, we present incident reports accepted during this quarter from quantitative perspectives such as statistics, as well as noteworthy cases.

1.1.1 Quarterly Statistical Information

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

JPCERT/CC received 14,056 incident reports this quarter. Of these, JPCERT/CC coordinated 3,398 cases with relevant organizations in Japan and overseas. The number of incident reports decreased by 8% from 15,345 in the previous quarter, while the number of cases coordinated increased

Table 1.1 Number of Incident Reports Related

Incident	Apr	May	Jun	Total	Last Qtr.
Number of Reports	5,432	4,770	3,854	14,056	15,345
Number of Incidents	3,691	2,201	3,413	9,305	10,262
Cases Coordinated	1,296	799	1,303	3,398	3,168

^{*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.

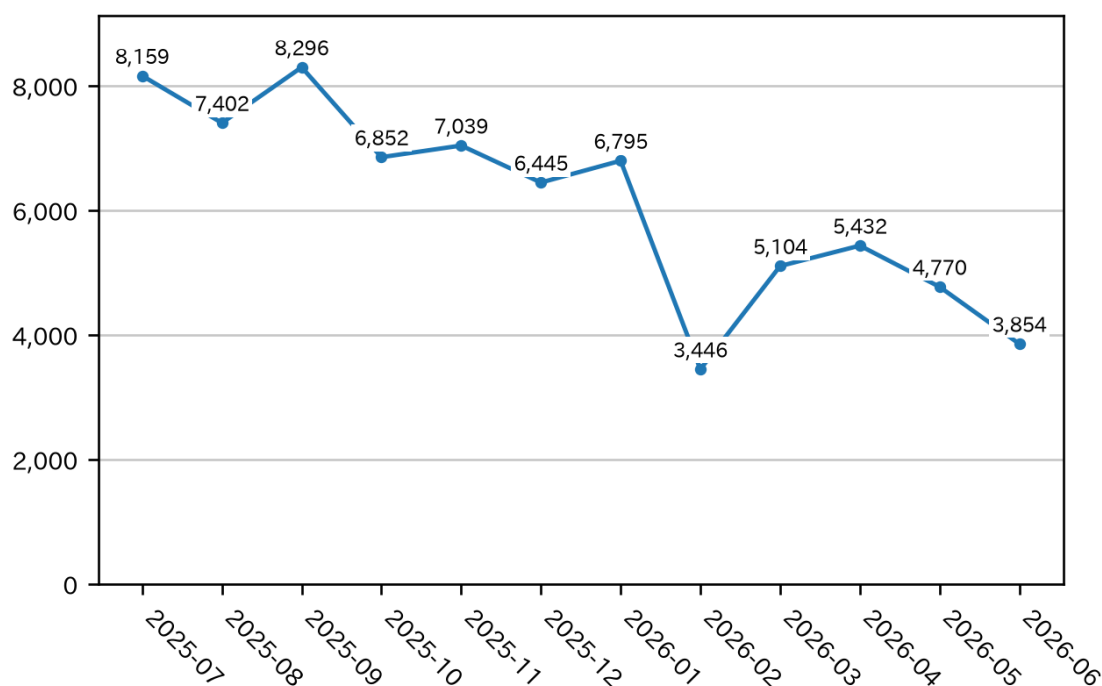


Figure 1.1 Trends in the Number of Incident Reports

by 7% from 3,168 in the previous quarter. The number of incident reports decreased by 3% from 14,558 in the same quarter last year, while the number of cases coordinated decreased by 4% from 3,544 in the same quarter last year.

The monthly trends over the past year for the number of reports and the number of cases coordinated 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 89.3%, while scan incidents, which search for system vulnerabilities, accounted for 2.0%.

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.

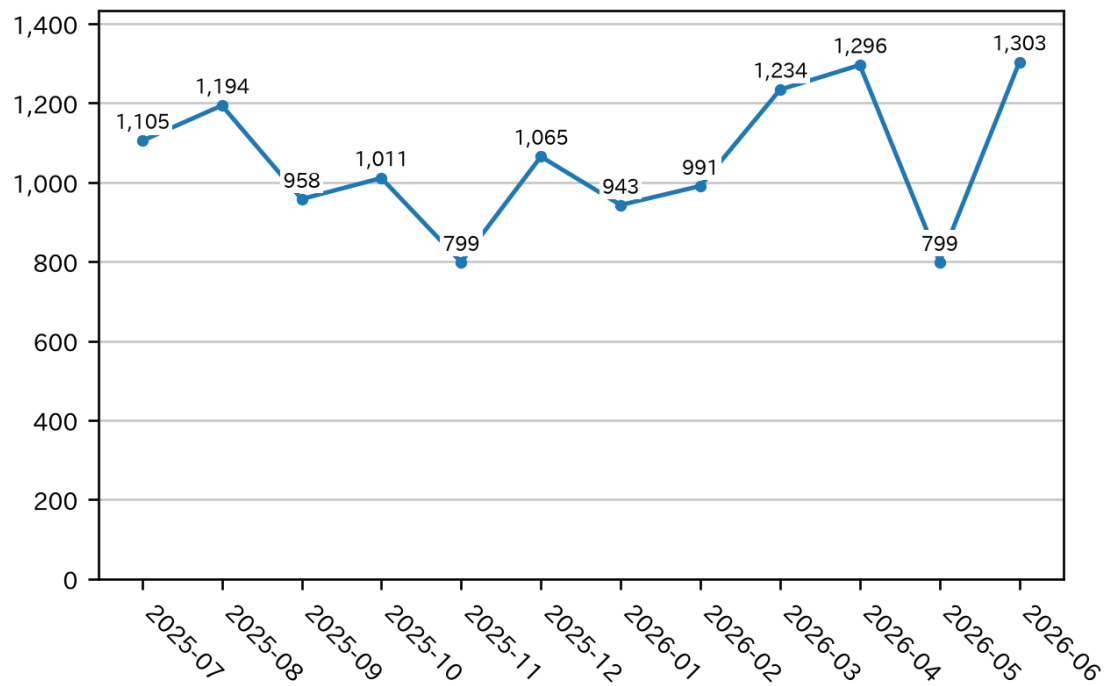


Figure 1.2 Trends in the Number of Cases Coordinated

Table 1.2 Number of Incident Reports by Category

Incident Category	Apr	May	Jun	Total	Last Qtr.
Phishing Site	3,352	1,928	3,033	8,313	9,293
Website Defacement	46	55	80	181	90
Malware Site	3	13	5	21	32
Scan	73	42	75	190	156
DoS/DDoS	1	0	0	1	4
Ransomware	3	3	2	8	0
ICS Related	0	1	0	1	0
Targeted Attack	3	4	1	8	2
Other	210	155	217	582	685

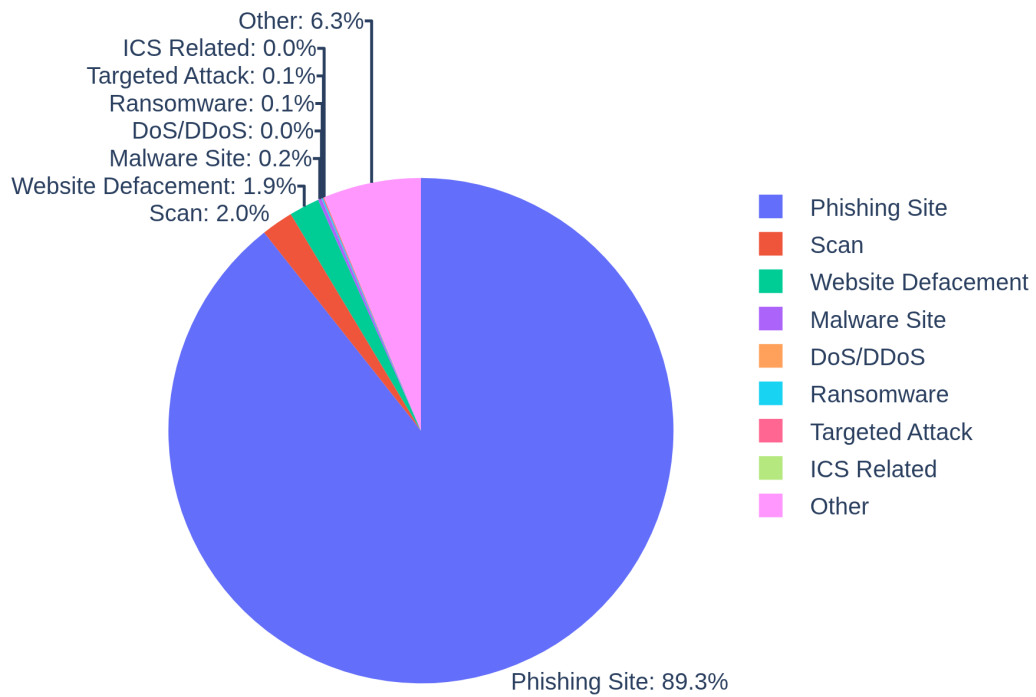


Figure 1.3 Percentage of the Number of Incident Reports by Category

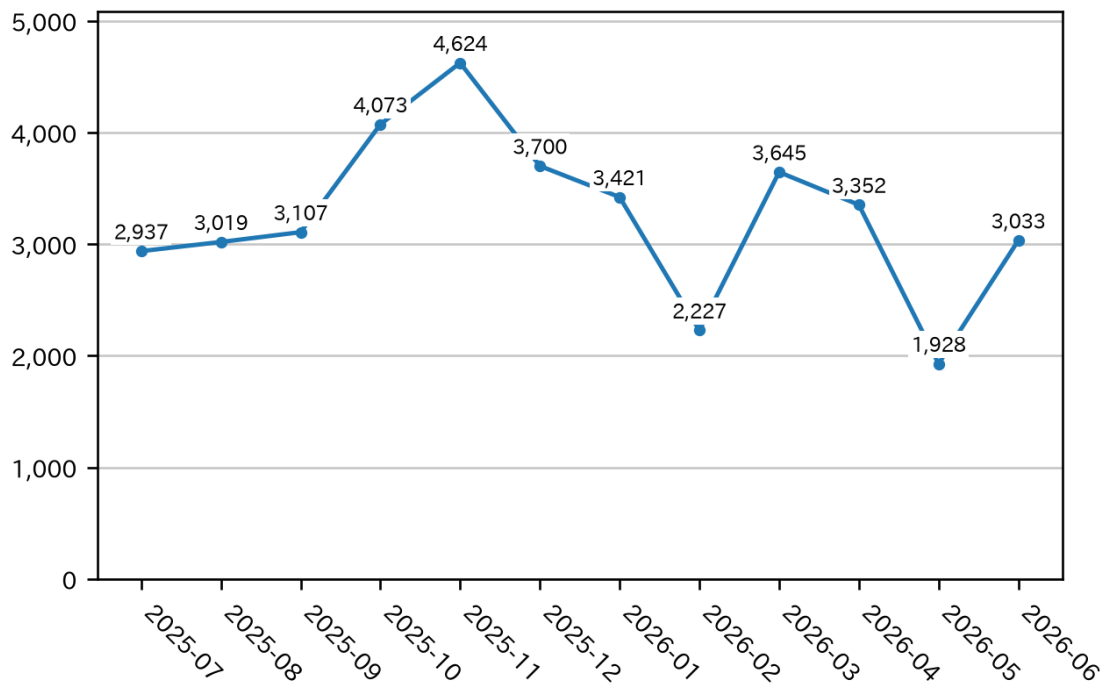


Figure 1.4 Trends in the Number of Phishing Sites

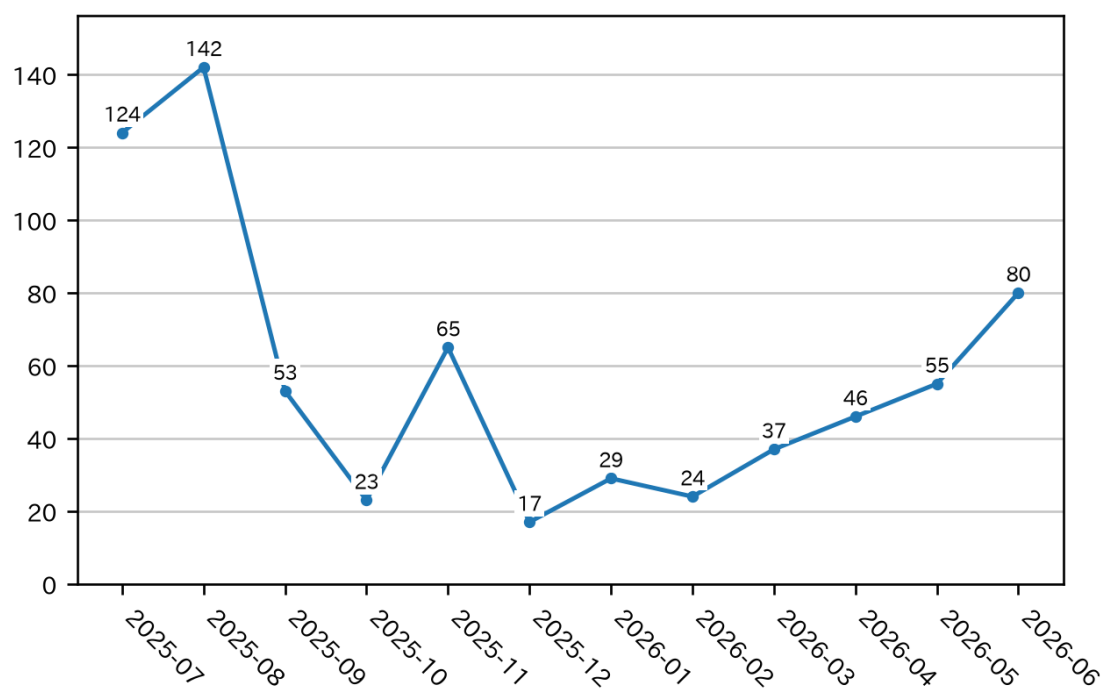


Figure 1.5 Trends in the Number of Website Defacements

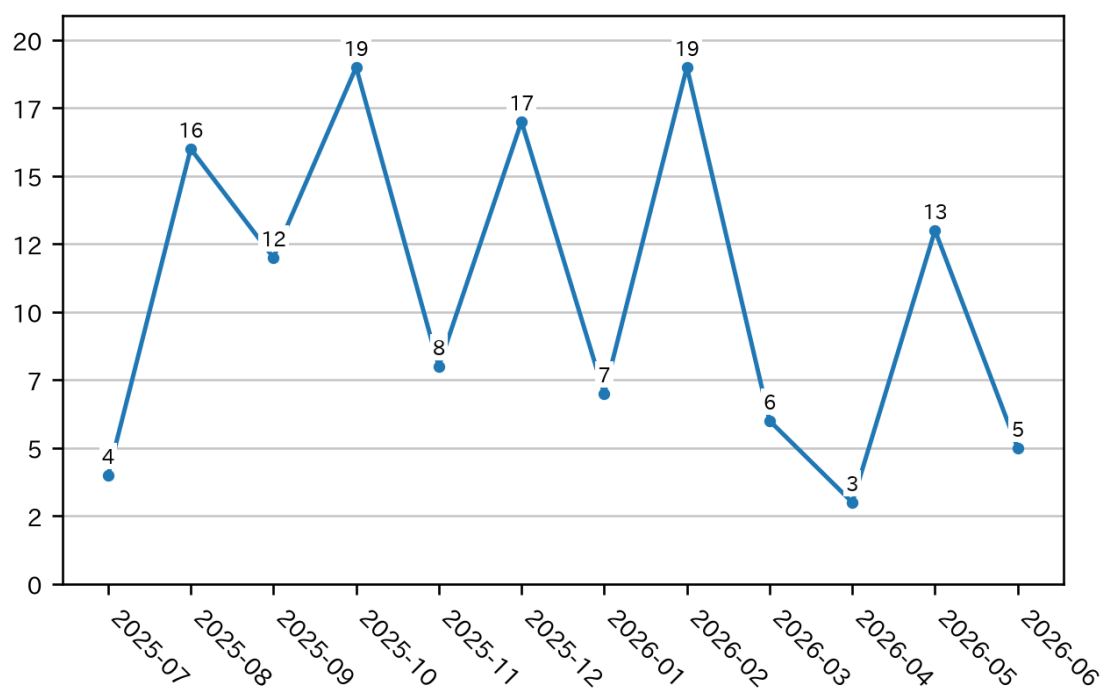


Figure 1.6 Trends in the Number of Malware Sites

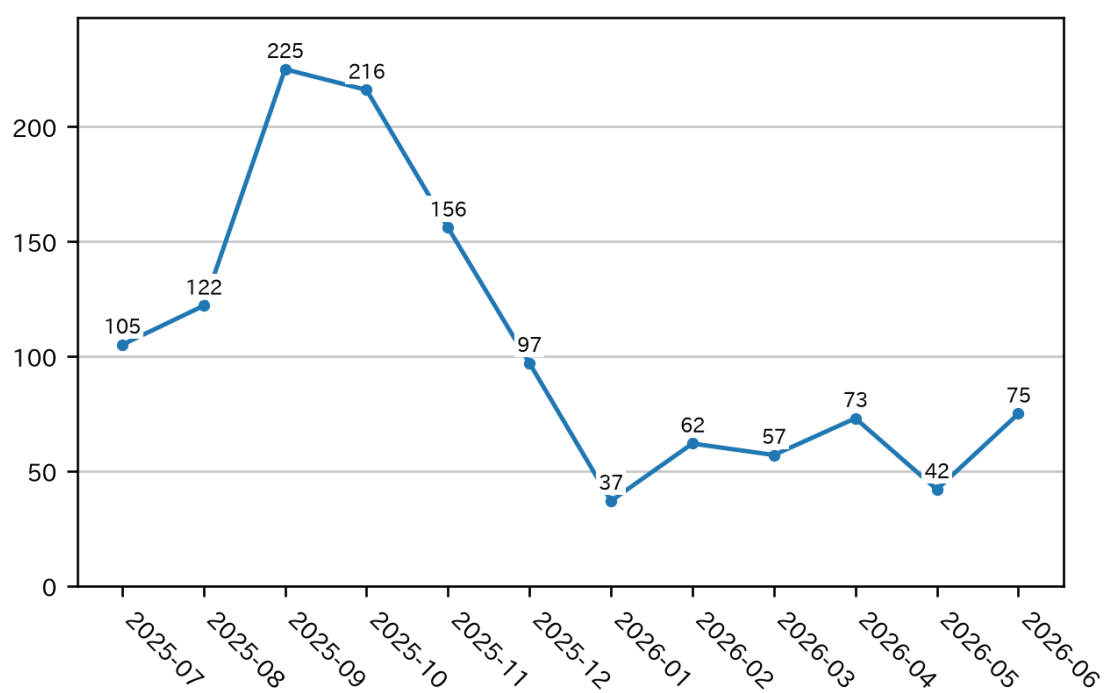


Figure 1.7 Trends in the Number of Scans

Table 1.3 Number of Phishing Sites for Domestic and Overseas Brands

Phishing Site	Apr	May	Jun	Total	Pct.
Domestic Brand	2,767	1,446	1,761	5,974	72%
Overseas Brand	239	217	632	1,088	13%
Unknown Brand	346	265	640	1,251	15%
Monthly Total	3,352	1,928	3,033	8,313	

1.1.2 Incident Trends

1.1.2.1 Trends in Phishing Sites

8,313 phishing sites were reported this quarter. The number of reported phishing sites decreased by 11% from 9,293 in the previous quarter and increased by 13% from 7,358 in the same quarter last year.

Of these, 1,088 phishing sites impersonated overseas brands; the number increased by 21% from 899 in the previous quarter. 5,974 phishing sites impersonated domestic brands; the number decreased by 16% from 7,112 in the previous quarter.

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 1.8 and Figure 1.9, respectively.

Of the phishing sites reported to JPCERT/CC, 50.7% of those related to overseas brands impersonated e-commerce sites, while 67.1% of those related to domestic brands impersonated financial sites. These were the largest shares in their respective groups.

For overseas brands, many phishing sites impersonated Amazon, Apple Account, and VISA. For domestic brands, many reports concerned phishing sites impersonating Saison Card, Monex, Inc., SBI Securities, Sumitomo Mitsui Card, and Rakuten.

Of the sites for which we coordinated takedown of phishing sites, 93% were overseas and 7% were domestic.

1.1.2.2 Trends in Website Defacement

181 website defacements were reported this quarter. The number of reported website defacements increased significantly by 101% from 90 in the previous quarter.

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

- Case 1: Overseas online casino content was displayed on legitimate websites

^{*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.

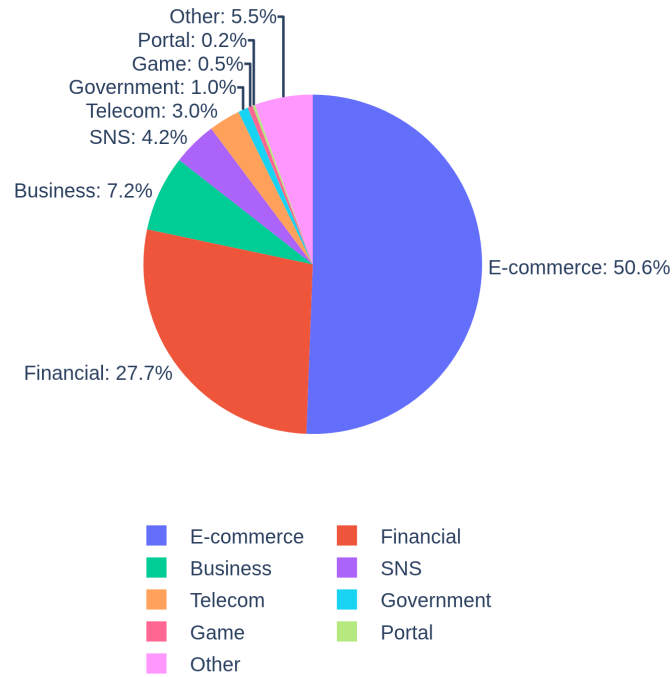


Figure 1.8 Percentage of the Number of Phishing Sites for Overseas Brands by Industry

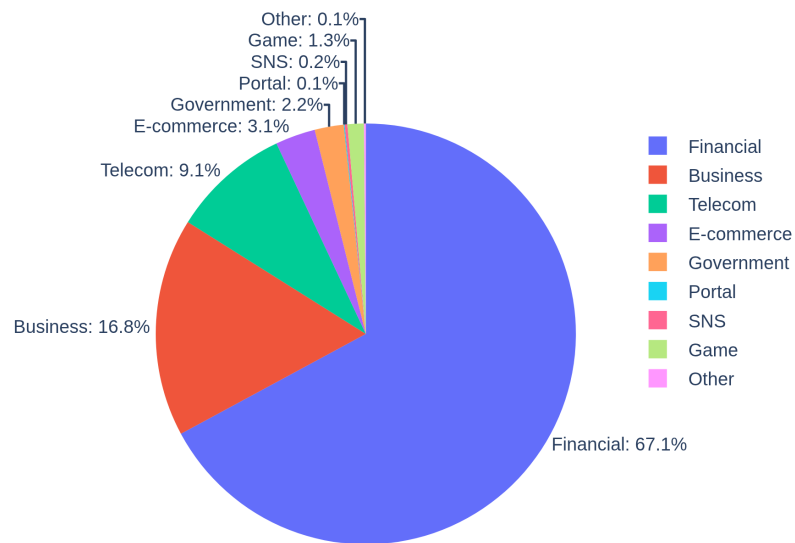


Figure 1.9 Percentage of the Number of Phishing Sites for Domestic Brands by Industry

- Case 2: A suspicious login page and a remote administration tool were installed on a legitimate website

In Case 1, multiple legitimate websites in Japan had been defaced, and overseas online casino content was displayed when the websites were accessed with the user agent used by search engines (Googlebot). This is considered to be SEO poisoning intended to make overseas online casino sites appear higher in search results.

In Case 2, a legitimate website in Japan had been defaced, and a suspicious login page had been

Table 1.4 Top 10 Ports by Number of Scans

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

placed on it. The site had been reported as a destination for voice phishing, which is thought to have been due to a login page placed by the attacker for the purpose of stealing Internet banking credentials. In addition, a remote administration tool had also been installed on the defaced website, and the attacker may have been attempting to remotely control users' devices separately from stealing credentials.

1.1.2.3 Trends in Targeted Attacks

8 incidents were classified as targeted attacks.

Targeted Attack Emails Abusing Legitimate Cloud Services

This quarter, JPCERT/CC received multiple reports of targeted attack emails that may have involved the attack group APT-C-60. Accessing the Proton Drive link provided in the targeted attack email caused a RAR file to be downloaded. Opening the LNK file contained in the RAR file downloaded malware from legitimate cloud services such as GitHub and GitLab, resulting in infection.

1.1.2.4 Trends in Other Incidents

21 malware sites were reported this quarter. The number of reported malware sites decreased by 34% from 32 in the previous quarter.

190 scan incidents were reported this quarter. The number of reported scan incidents increased by 22% from 156 in the previous quarter.

The top 10 most targeted ports for scans are shown in Table 1.4. Ports frequently targeted by scans were Telnet (23/TCP), HTTP (80/TCP), HTTPS (443/TCP), and 81/TCP.

582 incidents were classified as Other. The number of incidents classified as Other decreased by

15% from 685 in the previous quarter.

1.2 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.

1.2.1 Information Collection and Analysis

The information JPCERT/CC collects and analyzes includes not only information we gather ourselves but also information on incidents occurring in Japan and overseas that are reported to us, as well as 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 information sharing platform “CISTA (Collective Intelligence Station for Trusted Advocates)” (see 1.2.3) is effectively utilized, including sharing it with other organizations.

1.2.2 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 information distribution mailing list operated by JPCERT/CC (about 43,000 as of the end of this quarter).

1.2.2.1 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 or updated 12 Security Alerts. The following lists the information published or updated during the quarter in chronological order by the latest update date.

- 2026-04-13
Alert Regarding Vulnerabilities in Adobe Acrobat and Reader (APSB26-43)
- 2026-04-15
Microsoft Releases April 2026 Security Updates
- 2026-04-15
Alert Regarding Vulnerabilities in Adobe Acrobat and Reader (APSB26-44)
- 2026-04-27
Alert Regarding Multiple Vulnerabilities in Cisco ASA and FTD (CVE-2025-20333, CVE-2025-20362)
- 2026-05-13
Microsoft Releases May 2026 Security Updates
- 2026-05-13
Alert Regarding a Stack-based Buffer Overflow Vulnerability in GUARDIANWALL MailSuite
- 2026-05-21
Alert Regarding Multiple Vulnerabilities in Trend Micro Products Including TrendAI Apex One
- 2026-05-22
Alert Regarding an Authentication Bypass Vulnerability in Palo Alto Networks PAN-OS (CVE-2026-0265)
- 2026-06-10
Alert Regarding an Authentication Bypass Vulnerability in Check Point Software Technologies Products (CVE-2026-50751)
- 2026-06-10
Microsoft Releases June 2026 Security Updates
- 2026-06-10
Alert Regarding Vulnerabilities in Adobe Acrobat and Reader (APSB26-63)
- 2026-06-23
Alert Regarding Credential Leakage Related to Fortinet Products

1.2.2.2 Weekly Report

Among the security-related information collected by JPCERT/CC, we compile summaries of information deemed important and, in principle, publish them every Wednesday (the third business day of each week) as the “Weekly Report.”

This quarter, we published 12 items.

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

1.2.3 Information Provided via CISTA

JPCERT/CC operates CISTA, an information-sharing platform for threat intelligence, analysis, and countermeasure information related to cybersecurity, which is shared by cybersecurity-related departments of organizations, internal CSIRTs, and others. CISTA is a registration-based platform for organizations that support JPCERT/CC's initiatives.

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

- CISTA
<https://www.jpcert.or.jp/cista/>

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.

1.2.3.1 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 prompt dissemination to organizations that provide such infrastructure are shared as Early Warning Information.

This quarter, we issued 3 items.

1.2.3.2 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 61 items.

1.2.3.3 Indicator Information

For attack activities carried out against organizations in Japan that are considered to have targeted specific organizations or industries, JPCERT/CC provides Indicator Information to help detect such attacks. This information is provided with the permission of the relevant organizations for the purpose of identifying previously unrecognized damage and preventing damage.

This quarter, we provided 8 items.

1.2.3.4 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, we provided 38 items to organizations managing hosts affected by the vulnerabilities and threat information described above.

1.2.4 Response Cases

This section introduces notable cases from among the information collected this quarter, feedback received, information analyzed, and vulnerabilities and threat information coordinated and handled.

1.2.4.1 Authentication Bypass Vulnerability in cPanel and WHM (CVE-2026-41940)

WebPros International published an advisory^{*4} regarding an authentication bypass vulnerability (CVE-2026-41940) in cPanel and WHM on April 28, 2026. This vulnerability allows authentication to be bypassed in cPanel and WHM, and if exploited, an attacker can obtain root privileges for the products. When JPCERT/CC investigated the operational status of the products, it confirmed that approximately 2,000 hosts were operating in Japan and that a high percentage of the hosts were under the management of hosting providers. The products are often used by hosting providers to manage servers and other systems, and if they are adopted in a shared hosting environment, depending on the scope of compromise, all co-located tenants are highly likely to be affected. Therefore, we asked a community composed of hosting providers and others in which JPCERT/CC participates to check the status of their response.

On the day after the advisory was published, a security company released technical details^{*5} that included proof-of-concept code for this vulnerability. From two days after the advisory was published, information emerged in succession indicating that the vulnerability was being exploited in attacks that deploy Sorry ransomware and that distribute variants of Mirai malware^{*6*7}. Furthermore, it was also reported that the vulnerability had been exploited as a zero-day since February 2026, and based on the published proof-of-concept code, exploitation was considered to be easy. There were concerns that it would be exploited even more widely. JPCERT/CC also received a report from a domestic organization regarding damage caused by Sorry ransomware. The victim

^{*4} “WebPros International Security: CVE-2026-41940 - cPanel & WHM / WP2 Security Update 04/28/2026”. cPanel. <https://support.cpanel.net/hc/en-us/articles/40073787579671-Security-CVE-2026-41940-cPanel-WHM-WP2-Security-Update-04-28-2026>, (2026-04-28)

^{*5} “watchtowr The Internet Is Falling Down, Falling Down, Falling Down (cPanel & WHM Authentication Bypass CVE-2026-41940)”. watchTowr. <https://labs.watchtowr.com/the-internet-is-falling-down-falling-down-falling-down-cpanel-whm-authentication-bypass-cve-2026-41940/>, (2026-04-29)

^{*6} “The cPanel Situation Is...”. Censys. <https://censys.com/blog/the-cpanel-situation-is/>, (2026-05-01)

^{*7} “Critical cPanel flaw mass-exploited in ‘Sorry’ ransomware attacks”. Bleeping Computer. <https://www.bleepingcomputer.com/news/security/critical-cpanel-flaw-mass-exploited-in-sorry-ransomware-attacks/>, (2026-05-02)

organization used the products through services provided by the hosting provider as a tenant of that provider. The victim organization asked the provider to cooperate in a forensic investigation, but cooperation could not be obtained due to restrictions under the service contract, and a sufficient forensic investigation was not conducted. In addition, we received information^{*8} from an overseas organization with which JPCERT/CC collaborates that approximately 80 domestic hosts using the products were conducting suspicious communications. For these hosts, considering the possibility that they were affected by this vulnerability, we individually notified the relevant organizations and urged them to address the vulnerability.

1.2.4.2 Stack-Based Buffer Overflow Vulnerability in GUARDIANWALL MailSuite (CVE-2026-32661)

JPCERT/CC received a report regarding a vulnerability in GUARDIANWALL MailSuite, an integrated enterprise email security solution provided by Canon Marketing Japan. The report stated that an incident had occurred in the environment of a user of the product, and that the vulnerability had been discovered during the investigation. If a crafted request is sent to the product's web service, this vulnerability could allow arbitrary code to be executed without authentication, which could lead to compromise from outside via the Internet. There were concerns that the number of organizations affected by attacks exploiting this vulnerability could increase. Therefore, to distribute information on measures to prevent the spread of damage and information regarding the attacks, JPCERT/CC coordinated with the reporter and the product developer. For details on vulnerability coordination, see 3.1.2.1. On May 13, 2026, when the product developer published vulnerability information (CVE-2026-32661)^{*9}, JPCERT/CC published a JVN advisory^{*10} and released a Security Alert^{*11}. The Security Alert urged organizations using the affected product to apply the patch, and, taking into account the possibility that they may already have been compromised, to check whether they had been compromised, preserve necessary logs, and implement workarounds. In addition, JPCERT/CC shared the information regarding the attacks provided by the reporter as indicator information with organizations using CISTA, for the purpose of supporting user organizations in conducting investigations and assessing damage.

1.2.4.3 Authentication Bypass Vulnerability in Cisco Catalyst SD-WAN Controller (CVE-2026-20182)

On May 14, 2026, Cisco published an advisory^{*12} regarding an improper authentication vulnerability in Cisco Catalyst SD-WAN Controller (CVE-2026-20182). This vulnerability is an authentication

^{*8} "ShadowServer HIGH: Darknet Events Report". <https://www.shadowserver.org/what-we-do/network-reporting/honeypot-darknet-events-report/>

^{*9} "About the Stack-Based Buffer Overflow Vulnerability in GUARDIANWALL MailSuite". Canon IT Solutions Inc. https://security-support.canon-its.jp/info_and_news/show/804?site_domain=GUARDIANWALL, (2026-05-13)

^{*10} "JVN#35567473: Stack-Based Buffer Overflow Vulnerability in GUARDIANWALL MailSuite". Japan Vulnerability Notes. <https://jvn.jp/jp/JVN35567473/>, (2026-05-13)

^{*11} "Alert Regarding Stack-Based Buffer Overflow Vulnerability in GUARDIANWALL MailSuite". JPCERT Coordination Center (JPCERT/CC). <https://www.jpcert.or.jp/at/2026/at260013.html>, (2026-05-13)

^{*12} "Cisco Catalyst SD-WAN Controller Authentication Bypass Vulnerability". Cisco. <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-rpa2-v69WY2SW>, (2026-05-14)

bypass vulnerability in Cisco Catalyst SD-WAN Controller, and the advisory mentioned that exploitation of this vulnerability had already been observed at the time of publication. By exploiting this vulnerability, attackers may log in to Cisco Catalyst SD-WAN Controller as a non-root user account with high internal privileges.

In addition, logs indicating completion of authentication when an attacker bypasses authentication and establishes a connection are recorded in the same format as those for a legitimate peer, so it may be difficult to detect compromise by checking logs alone. Attackers may use the established non-root user account to access NETCONF and, as a result, manipulate the network configuration of the SD-WAN fabric.

Regarding this product, an authentication bypass vulnerability (CVE-2026-20127) was also published in February 2026, and Cisco Talos' investigation estimates that zero-day exploitation had continued since 2023. JPCERT/CC anticipated that attackers would continue to target this product and conducted an investigation to identify hosts in Japan that were exposed to the Internet while affected by this vulnerability. However, the service affected by this vulnerability is used for control connections between SD-WAN devices, and because distinctive responses such as Web responses and banners are difficult to obtain, scanning services cannot comprehensively capture the operating status of this product. Since there are limitations to understanding the actual situation, the investigation results were supplemented by working with Cisco to understand the use of the product in Japan.

In addition, Cisco published an advisory^{*13} on June 4, 2026, for an authenticated privilege escalation vulnerability in Cisco Catalyst SD-WAN Manager (CVE-2026-20245), suggesting an attack scenario in which an unauthenticated attacker gains privileges on the product through chained exploitation with other vulnerabilities, including CVE-2026-20182.

JPCERT/CC received a report from an organization in Japan on a case involving compromise of the product and supported the investigation. As a result of analyzing information received from the organization and logs from the compromised devices, JPCERT/CC confirmed traces in logs as of April 2026 indicating the possibility that an attacker had exploited CVE-2026-20245. We also confirmed traces of the addition of an administrator account, login to the Web UI of internal network routers using the created administrator privileges, and configuration change operations. The indicator information obtained from the analysis was returned to the organization and shared with international communities with which JPCERT/CC collaborates, among others.

^{*13} "Cisco Catalyst SD-WAN Manager Authenticated Privilege Escalation Vulnerability". Cisco. <https://sec.cloudapps.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-sdwan-privesc-4uxFrDzx>, (2026-06-04)

Chapter 2

Observation and Analysis of Reconnaissance and Attack Activities on the Internet

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

2.1 Monitoring Using the Internet Threat Monitoring System “TSUBAME”

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

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>

2.1.1 Utilization of TSUBAME Observation Data

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

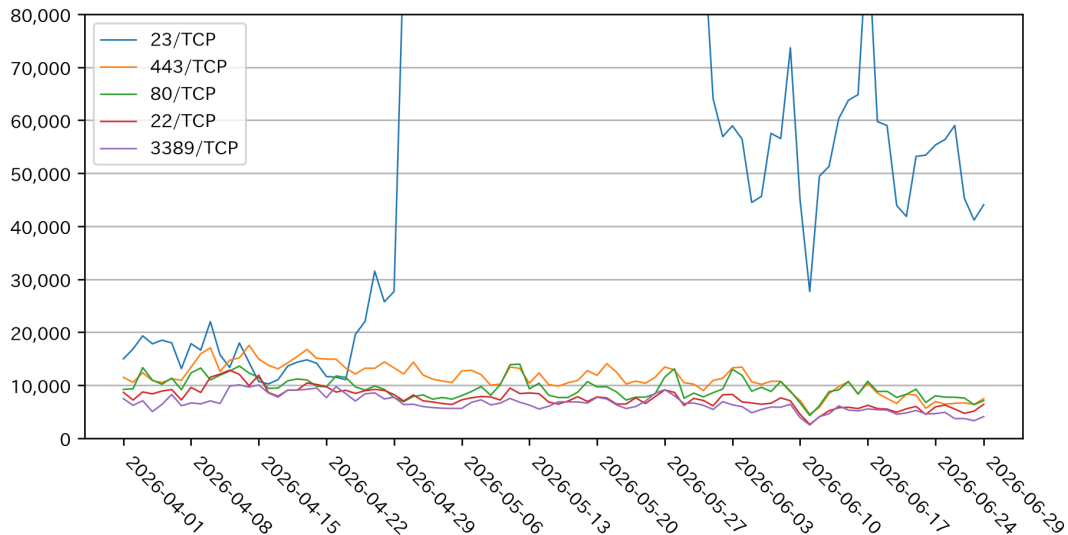


Figure 2.1 Packet Counts for Top 1-5 Destination Ports Observed by TSUBAME

itoring Report and the blog “TSUBAME Report Overflow” on a quarterly basis. Starting with this quarter, the content previously provided in the Internet Threat Monitoring Report is included in Chapter 2, “Observation and Analysis of Reconnaissance and Attack Activities on the Internet,” of this report. The blog “TSUBAME Report Overflow” will continue to cover analysis that cannot be fully included in this report and notable events that occurred during the period.

- JPCERT/CC Internet Threat Monitoring Report
 - Internet Threat Monitoring Report (January–March 2026)
<https://www.jpcert.or.jp/tsubame/report/report202601-03.html>
- TSUBAME Report Overflow
 - TSUBAME Report Overflow (October–December 2025)
<https://blogs.jpcert.or.jp/ja/2026/05/tsubame-overflow20251012.html>
 - TSUBAME Report Overflow (January–March 2026)
<https://blogs.jpcert.or.jp/ja/2026/06/tsubame-overflow20260103.html>

2.1.2 TSUBAME Observation Trends

Figure 2.1 shows an aggregation by destination port of the number of packets received by TSUBAME sensors in Japan this quarter^{*1}. Please refer to this when analyzing trends in packets reaching an organization’s network.

The most frequently observed packets this quarter were to 23/TCP (Telnet). A sudden increase in packets with characteristics of Mirai was observed in early May 2026, but the number has gradually decreased since then. 443/TCP ranked second. 80/TCP ranked third and 22/TCP ranked fourth,

^{*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.

Table 2.1 Top Five Frequently Scanned Domestic Services (Destination Port Numbers)

Rank	Destination Port Number	Rank in Previous Quarter
1	Telnet (23/TCP)	1
2	https (443/TCP)	3
3	http (80/TCP)	2
4	ssh (22/TCP)	5
5	rdp (3389/TCP)	6

Table 2.2 Top Five Scan Source Regions

Rank	Scan Source Region	Rank in Previous Quarter
1	United States (US)	1
2	Netherlands (NL)	4
3	United Kingdom (GB)	8
4	Germany (DE)	6
5	Romania (RO)	7

swapping positions from the previous quarter. 3389/TCP ranked fifth. The top five frequently scanned domestic services (destination port numbers) are shown in Table 2.1, and the top five scan source regions are shown in Table 2.2.

Trends in the number of observed packets scanning the services shown in Table 2.1 are shown in Figure 2.1.

The top five scan source regions for scan activities targeting Japan, listed in order of activity during this quarter, are shown in Table 2.2.

The United States was the top region, followed by the Netherlands. The regions ranked third and lower were the United Kingdom, Germany, and Romania, all of which had ranked outside the top five in the previous quarter. Note that TSUBAME determines the region of each IP address using allocation information from RIRs (Regional Internet Registries).

2.2 Honeypot Operation and Analysis

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

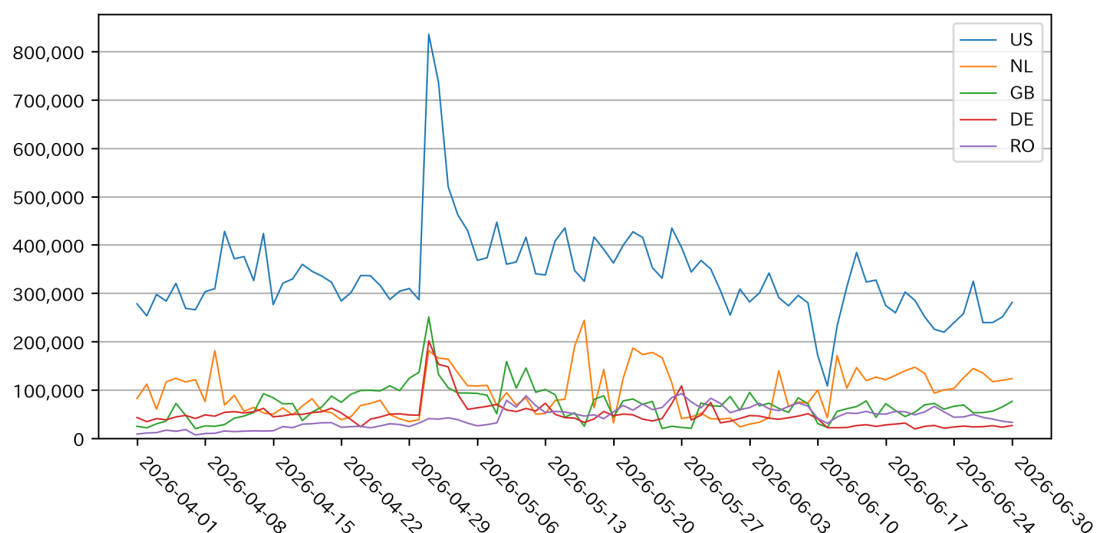


Figure 2.2 Packet Count Trends by Scan Source Region

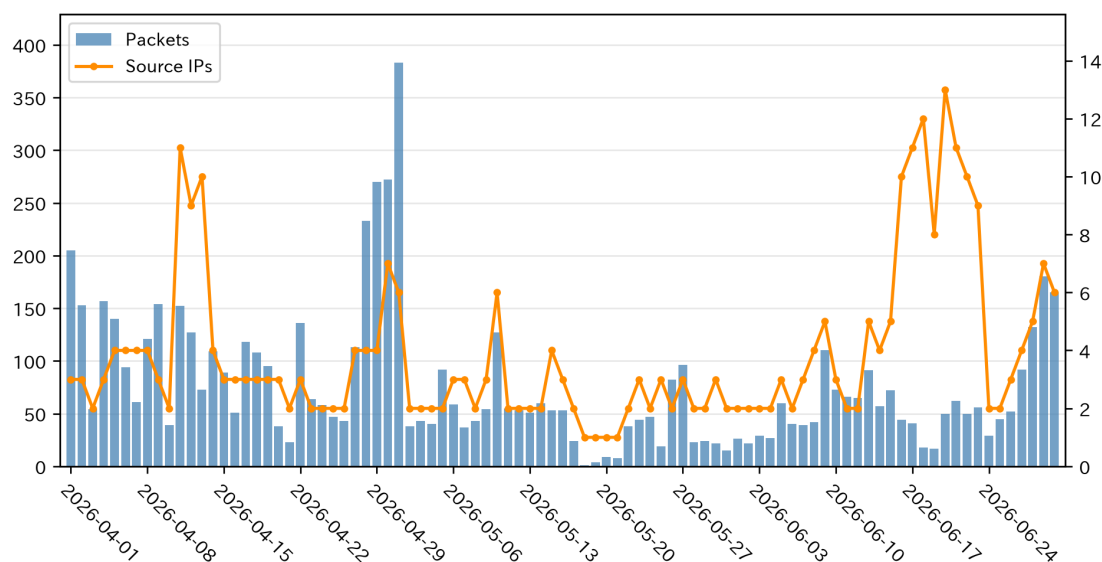


Figure 2.3 Observed Attack Activity Targeting CVE-2025-55182

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

Following the previous quarter, attack packets targeting a vulnerability in React Server Components (CVE-2025-55182) have been continuously observed (Figure 2.3).

Multiple variations have been observed in the attack code contained in the payloads, suggesting that attackers are continuing to improve it. Attack activity exploiting this vulnerability is likely to continue, and continued caution is required.

2.2.2 Communications Targeting Vulnerabilities in LLM-Related Frameworks

Attack packets and scan packets targeting vulnerabilities in frameworks and libraries that work with LLMs, such as a code execution vulnerability in n8n (CVE-2026-21858) and code execution vulnerabilities in llama-cpp-python / SGLang (CVE-2024-34359 / CVE-2026-5760), have been sporadically observed since around late April 2026.

Development platforms that work with LLMs are considered relatively likely to have communication paths to the Internet. In addition to applying vulnerability fixes, it is important to implement measures with defense in depth in mind, such as appropriately controlling communications.

Chapter 3

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 Innovation Platform 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.

3.1 Handling Status of Vulnerability-Related Information

3.1.1 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.

3.1.2 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 “JNVNU#” followed by 8 digits; e.g., JNVNU#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, 111 vulnerability advisories were published on JVN, bringing the cumulative total to 6,095. The cumulative trend is shown in Figure 3.1.

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

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

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

- Vulnerability information reported under the Partnership Guideline: 44
- Vulnerability information based on international or independent coordination: 67
- Technical information related to vulnerabilities: 0

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

- Innovation Platform Agency, Japan (IPA): Status of Reports Concerning Vulnerability-related Information for Software, etc.
<https://www.ipa.go.jp/security/reports/vuln/software/index.html>

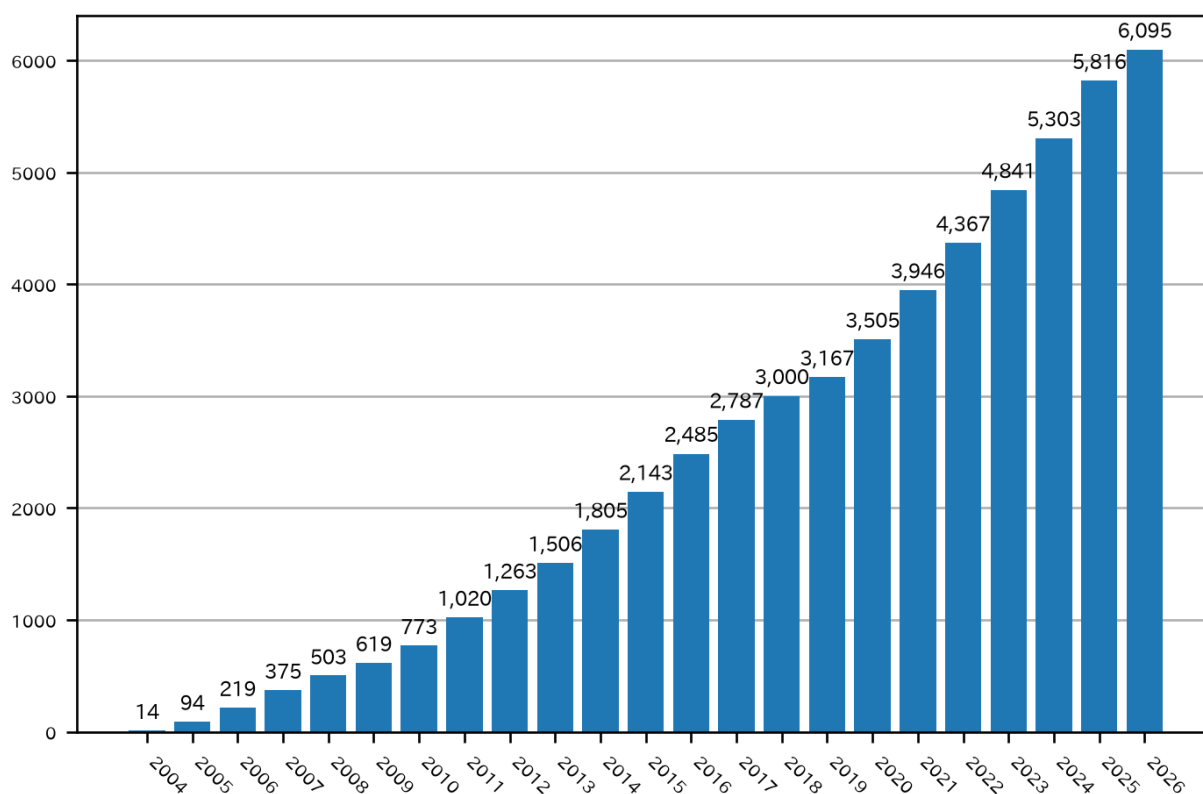


Figure 3.1 Cumulative Number of JVN Publications

3.1.2.1 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#35567473 Stack-Based Buffer Overflow Vulnerability in GUARDIANWALL MailSuite

- JVN#35567473 Stack-Based Buffer Overflow Vulnerability in GUARDIANWALL MailSuite
<https://jvn.jp/jp/JVN35567473/>

This is a vulnerability in “GUARDIANWALL MailSuite,” an integrated email security solution for enterprises provided by Canon Marketing Japan Inc. This product is used by many organizations in Japan, including public institutions and companies responsible for operating critical infrastructure.

This vulnerability was reported by the product developer as a vulnerability discovered during the investigation of an incident that occurred in a product user’s environment. The vulnerability allows an attacker to cause a stack-based buffer overflow and execute arbitrary code without authentication by sending a crafted request. If exploited, it could have a serious impact on confidentiality, integrity, and availability, and could lead not only to confusion among users but also to more significant damage. Since exploitation of this vulnerability had been confirmed in a product user’s environment,

when publishing the JVN advisory, we marked the title as “Urgent” and stated in the details that exploitation had been confirmed, urging organizations to respond promptly. After publishing the advisory, we also issued a Security Alert related to this matter to call for further caution among users. For the Security Alert, please refer to 1.2.4.2.

JVN#00263243, JVN#57877356 Handling of Vulnerabilities in Tools Provided by JPCERT/CC (EmoCheck, LogonTracer)

- JVN#00263243 DLL Loading Vulnerability in EmoCheck
<https://jvn.jp/jp/JVN00263243/>
- JVN#57877356 Multiple Vulnerabilities in LogonTracer
<https://jvn.jp/jp/JVN57877356/>

Both advisories provide information on vulnerabilities in tools provided by JPCERT/CC. JPCERT/CC received the reports through the Information Security Early Warning Partnership and, as the product developer, fixed the vulnerabilities and disseminated related information. EmoCheck, for which a DLL loading vulnerability was reported, is a tool released in February 2020 to check for infections in order to counter the spread of Emotet infections that occurred around 2019. Since the threat of Emotet no longer exists, JPCERT/CC took the vulnerability report as an opportunity to end distribution and call on users to stop using the tool. For LogonTracer, a tool that supports analysis of event logs, JPCERT/CC released v2.0, which addresses the vulnerabilities. JPCERT/CC will make use of this response in its future activities and continue aiming for higher-quality coordination while working closely with product developers.

3.1.2.2 Notable Vulnerabilities Handled via International or Independent Coordination

There were no notable vulnerabilities this quarter.

3.1.2.3 Other Notable Matters Related to Vulnerability Coordination

We introduce changes to the format of Japanese advisories published on JVN based on security advisories published by overseas vendors and CERT organizations.

JVNVU#96777324 Updates for Intel Products (May 2026)

- JVNVU#96777324 Updates for Intel Products (May 2026)
<https://jvn.jp/vu/JVNVU96777324/>

JPCERT/CC has previously translated into Japanese information issued by Intel, Siemens, Apache and other OSS projects, as well as CERT/CC and CISA ICS in the United States, and published it on JVN as advisories with the identifier “JVNVU#” followed by 8 digits. However, with the widespread adoption of automatic translation services, JVN has stopped including Japanese translations of

advisory details and changed to a simplified format that focuses on notifications when advisories are published or updated. This format has been applied gradually since March 2026, and its scope was expanded this quarter; Intel advisories published in May 2026 use this simplified format. By flexibly reviewing advisory formats in response to changes in readers' usage environments and other factors, JVN aims to deliver useful information more quickly.

3.1.3 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/>

3.1.4 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 65 vulnerabilities.

For CNAs and CVE, please refer to the following web page.

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

3.2 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.

- To Everyone Handling Vulnerability-related Information in Japan: Request for Responses in Accordance with the Information Security Early Warning Partnership Guideline
https://www.meti.go.jp/policy/netsecurity/vul_request.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>

3.2.1 Collaboration with Product Developers in Japan

As a coordination center, JPCERT/CC maintains a list of product developers who are recipients of vulnerability information. Product developers are asked to register, and as of the end of this quarter, the number of registrations was 1,364, as shown in Figure 3.2.

For details, please refer to the following web page.

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

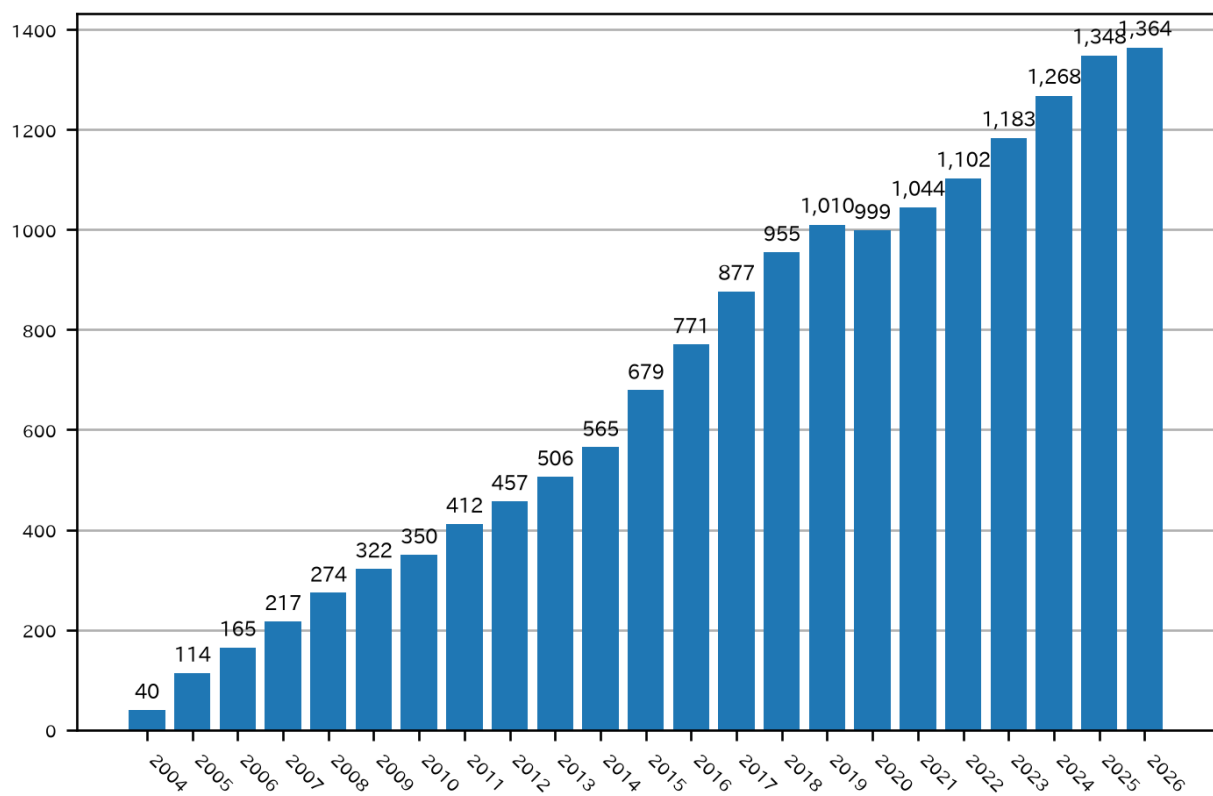


Figure 3.2 Number of Registered Product Developers

Chapter 4

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.

4.1 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.

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

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

4.1.2 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 84th CEPTOAR Council Steering Committee held on June 8, 2026, we shared information about the status of recent software supply chain attack cases and countermeasures.

4.2 Strengthening Collaboration and Establishing Information Exchange Environments with Domestic Stakeholders

4.2.1 Promoting Collaboration with CISTA Users

For CISTA users, in addition to information sharing activities through CISTA, 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 user organizations to stimulate dialogue.

Note that this quarter, we registered 27 new organizations as CISTA users.

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

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

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

4.3 Provision of Information and Tools

4.3.1 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 5

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.

5.1 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.

5.2 International CSIRT Collaboration

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

5.2.1 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/>

5.2.1.1 Holding of the APCERT Steering Committee Meeting

The APCERT Steering Committee held an in-person meeting in Kuala Lumpur, Malaysia, on April 8, 2026, and a teleconference on June 30, 2026, to discuss APCERT's operational policies and other matters. JPCERT/CC participated in the meetings as a Steering Committee member and also supported meeting operations as the Secretariat.

5.2.2 FIRST (Forum of Incident Response and Security Teams)

Since joining in 1998, JPCERT/CC has actively participated in FIRST activities. Since June 2021, Yukako Uchida of the Global Coordination Division has served on the Board and this quarter participated in the monthly online Board meetings, as well as the in-person Board meetings held in Munich, Germany in April 2026 and Denver, United States in June 2026.

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

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

5.2.2.1 Participation in the 38th Annual FIRST Conference

The 38th Annual FIRST Conference was held from June 14 to June 19, 2026, in Denver, United States. This meeting is held annually to exchange information on the latest trends in cyber incident prevention, response, technical analysis, etc., and to strengthen collaboration among incident response teams. This year, a wide variety of topics were covered under the theme “Peak Defense: Building Adaptive Systems for Modern Threats,” and approximately 700 people from various countries participated in person. During the conference, JPCERT/CC held individual discussions with National CSIRTs from around the world, CSIRTs of product vendors, and others. Through participation in such meetings, JPCERT/CC will continue working to strengthen collaboration by promoting information sharing and building relationships of trust with relevant organizations in each region, so that international incident response coordination can be carried out more smoothly. For details about the 38th Annual FIRST Conference, please refer to the following web page.

- 38th ANNUAL FIRST CONFERENCE
<https://www.first.org/conference/2026/>

5.3 Visits to and from Overseas CSIRTs, etc.

Through visits to and from overseas CSIRTs, JPCERT/CC discusses with them and exchanges views on future collaboration. This quarter, the following visits to and from organizations took place.

- Visit to CyberSecurity Malaysia (April 9, 2026)
- Visit from CERT-EU (May 26, 2026)

5.4 Participation in Other International Conferences

5.4.1 Participation in Locked Shields

From April 20 to April 24, 2026, JPCERT/CC participated online in Locked Shields 2026, an international cyber exercise hosted by the NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE). Five JPCERT/CC staff members worked as part of a Blue Team together with participants from the Japanese government and critical infrastructure operators to handle incident response and legal and public relations challenges.

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

5.4.2 Participation in NatCSIRT 2026

The National CSIRT Meeting (NatCSIRT) 2026, hosted by CERT/CC in the United States, was held in Denver, United States, on dates immediately following the 38th Annual FIRST Conference. This meeting is held annually to bring together National CSIRTs from around the world to share activity plans and challenges as incident response teams representing their countries, and to present and discuss development tools, joint projects, research, and other topics. At this meeting, JPCERT/CC joined a panel discussion on the use of AI in incident response and introduced examples of improving operational efficiency using AI. For details on NatCSIRT, please refer to the following web page.

- NatCSIRT 2026
<https://resources.sei.cmu.edu/news-events/events/natcsirt/index.cfm>

5.5 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, work proceeded on preparing the second Working Draft (WD2) for both ISO/IEC 29147 (Vulnerability disclosure) and ISO/IEC 30111 (Vulnerability handling processes), which were under revision, based on the decisions made at the international meeting in March 2026.

As a result, the WD2 was completed and sent to the SC 27 Secretariat with a request that it be distributed to the participating countries. Going forward, experts in each country are expected to submit comments on the WD2, and how to address those comments is scheduled to be considered at the international meeting this fall.

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

JPCERT/CC has established cooperative relationships with organizations responsible for vulnerability coordination in regions around the world and works with them on coordination of international activities and information sharing, among other matters. In addition, JPCERT/CC participates in international community activities related to vulnerabilities, including FIRST, and works to build a foundation for collaboration.

5.6.1 Participation in CVE/FIRST VulnCon 2026 & Annual CNA Summit

From April 13 to April 16, 2026, CVE/FIRST VulnCon 2026 & Annual CNA Summit, jointly hosted by FIRST and the CVE Program, was held in Scottsdale, Arizona, United States. JPCERT/CC planned and conducted, as a facilitator, a tabletop exercise that included discussions on methods related to Coordinated Vulnerability Disclosure (CVD). It also operated a meeting of the Global Community of Practice on Coordinated Vulnerability Disclosure (CVD-COP), an international community of vulnerability coordinator organizations established in 2024 under the leadership of CISA in the United States, in which JPCERT/CC also collaborates as a co-chair. At the meeting, presentations and information sharing on the status of activities and future issues, as well as exchanges of views, were conducted. For details on the event, please refer to the following web page.

- CVE/FIRST VulnCon 2026 & Annual CNA Summit
<https://www.first.org/conference/vulncon26/>

Chapter 6

Council of Anti-Phishing Japan Activities

The Council of Anti-Phishing Japan (hereinafter in this chapter, the “Council”) is a membership organization that collects and provides information on phishing, analyzes trends, and examines technical and institutional responses. JPCERT/CC, commissioned by the Ministry of Economy, Trade and Industry, handles acceptance of phishing reports and inquiries from general consumers, publishes Security Alerts about phishing sites, and operates certain working groups as part of the Council’s activities.

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

Besides activities commissioned by the Ministry of Economy, Trade and Industry, the Council conducts its own activities for member organizations based on decisions of the Steering Committee, and JPCERT/CC, as the Secretariat, also supports the implementation of these activities. Specifically, see “Section 6.2 Activities for Member Organizations of the Council of Anti-Phishing Japan.”

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

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

6.1.1 Acceptance of Phishing Reports and Inquiries

Although the figure for this quarter has not yet been finalized, the number of phishing reports is expected to continue decreasing from the previous quarter. Phishing related to securities services, which was frequently reported in April 2026, decreased from May 2026 onward. Meanwhile, a technique that has been reported since March 2026, in which attackers impersonate payment requests for National Health Insurance, resident tax, National Pension, and other payments and have victims send money directly using the PayPay app, increased (Figure 6.1).

The trend in the number of phishing reports over the past year is shown in Figure 6.2.

By breakdown of reports, those impersonating Amazon were the most numerous, accounting for

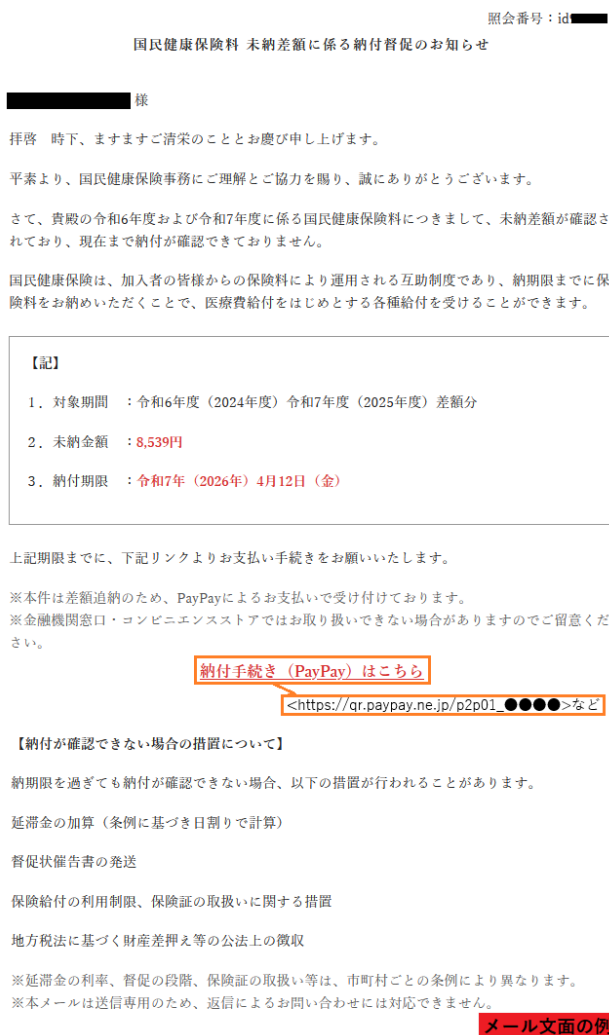


Figure 6.1 Example of a Phishing Email Leading to PayPay

about 13.9% of the total. This was followed by reports of phishing impersonating Rakuten Card, accounting for about 12.9% of the total.

6.1.2 Information Gathering and Distribution

6.1.2.1 Regular Reports

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

- Council of Anti-Phishing Japan Website
<https://www.antiphishing.jp/>
- 2026/03 Phishing Report Status
<https://www.antiphishing.jp/report/monthly/202603.html>
- 2026/04 Phishing Report Status

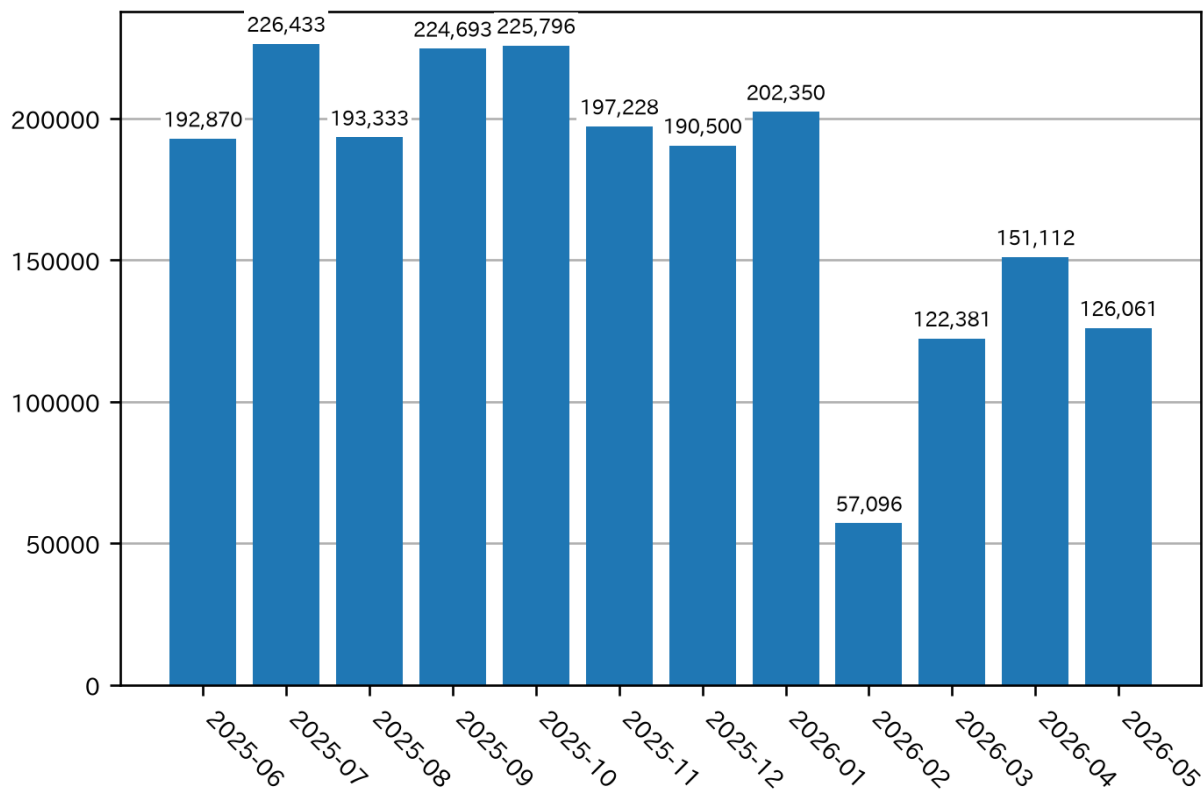


Figure 6.2 Number of Phishing Reports

<https://www.antiphishing.jp/report/monthly/202604.html>

- 2026/05 Phishing Report Status

<https://www.antiphishing.jp/report/monthly/202605.html>

6.1.2.2 Provision of Phishing Site URL Information

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

6.1.2.3 Publication of Anti-Phishing Guidelines and the Phishing Report

The “Technical and Institutional Study Working Group” is a working group composed of experts, primarily members of the Council, that creates and revises guidelines and trend reports on anti-phishing measures. On June 1, 2026, we published the “Anti-Phishing Guidelines 2026 Edition,” “Anti-Phishing Scam Countermeasures Guidelines for Users 2026 Edition,” and “Phishing Report 2026,” whose revision and creation had been advanced by the Technical and Institutional Study Working Group in the previous fiscal year. In addition to the existing PDF versions, they are also

posted as web pages in HTML format.

- Publication of Materials: Notice of Revision of Anti-Phishing Guidelines
<https://www.antiphishing.jp/news/info/guideline2026.html.html>
- Publication of Materials: Notice of Publication of Phishing Report 2026
https://www.antiphishing.jp/news/info/press-phishing_report2026.html

6.2 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.

6.2.1 Steering Committee Meetings

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

- 137th Steering Committee
Date: April 23, 2026
- 138th Steering Committee
Date: May 28, 2026
- 139th Steering Committee
Date: June 25, 2026

6.2.2 Support for Holding Working Group Meetings, etc.

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

- Research Working Group Meeting
Date: Every Tuesday from April 2026 to June 2026
- Certificate Promotion Working Group Meeting
Date: May 25, 2026
- Council of Anti-Phishing Japan FY2026 General Meeting
Date: June 17, 2026

Chapter 7

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.

7.1 Presentations

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

- be Connected Executive Roundtable: Cyber Resilience in the Age of Ransomware — Strengthening Incident Response Capabilities Through Interactive Discussions
Title: Preparing to Prevent Ransomware Attack Damage from Becoming the Norm
Presenter: Hayato Sasaki (Deputy Director, Threat Information Analyst, Cyber Security Coordination Group)
Organizer: BUSINESS FORUM NET. Co., Ltd.
Presentation date: May 20, 2026
- FY2026 General Meeting of the Municipal CSIRT Council
Title: Initial Response to Intrusive Ransomware Attacks
Presenter: Yuki Yano (Threat Analysis and Incident Response Team, Cyber Security Coordination Group)
Organizer: Secretariat of the Municipal CSIRT Council
Presentation date: May 27, 2026

7.2 Support and Sponsorship

This quarter, JPCERT/CC supported or sponsored the following events.

- 30th Shirahama Symposium on Cyber Crime

Organizer: Executive Committee of the Shirahama Symposium on Cyber Crime

Date: May 21, 2026 - May 23, 2026

- Interop Tokyo 2026

Organizer: Interop Tokyo Executive Committee

Date: June 10, 2026 - June 12, 2026

- Edge AI Initiative 2026

Organizer: ITmedia Inc.

Date: June 16, 2026 - June 18, 2026

7.3 Published Materials

This quarter, we published the following materials.

7.3.1 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 have compiled the results of such Internet monitoring each quarter and published them in Japanese and English as the “Internet Threat Monitoring Report,” but that report ended with the following issue for the fourth quarter of FY2025 and has been integrated into this report. Going forward, please refer to **Chapter 2 Observation and Analysis of Reconnaissance and Attack Activities on the Internet** in this report.

- 2026-05-15

JPCERT/CC Internet Threat Monitoring Report [January 1, 2026 - March 31, 2026]

<https://www.jpcert.or.jp/tsubame/report/report202601-03.html>

- 2026-06-17

JPCERT/CC Internet Threat Monitoring Report [January 1, 2026 - March 31, 2026]

<https://www.jpcert.or.jp/english/tsubame/report/report202601-03.html>

7.3.2 Status of Reports on Software Vulnerability-Related Information

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

quarter and notable trends in vulnerabilities disclosed during the same period.

- 2026-04-16

Status of Reports on Software Vulnerability-Related Information [Q1 2026 (January–March)]

https://www.jpcert.or.jp/pr/2026/vulnREPORT_2026q1.pdf

7.3.3 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 5 articles.

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

- 2026-05-13

TSUBAME Report Overflow (Oct-Dec 2025)

- 2026-06-02

TSUBAME Report Overflow (Jan-Mar 2026)

- 2026-06-11

Update to the Tool Analysis Result Sheet

English articles: 2 articles <https://blogs.jpcert.or.jp/en/>

- 2026-04-14

ICS Security Conference 2026

- 2026-05-14

TSUBAME Report Overflow (Oct-Dec 2025)

Appendix A

Incident Categories

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

Phishing Site

Phishing site refers to a site used for “phishing scams” that impersonate legitimate sites of service providers such as banks and auctions to trick users into divulging information such as IDs, passwords, and credit card numbers.

At JPCERT/CC, the following are classified as **phishing sites**.

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

Website Defacement

Website defacement refers to a site where the website content has been altered by an attacker or malware (including the insertion of scripts not intended by the administrator).

At JPCERT/CC, the following are classified as **website defacement**.

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

Malware Site

Malware site refers to an attack site that infects a PC with malware upon viewing, or a site that publishes malware used in attacks.

At JPCERT/CC, the following are classified as **malware sites**.

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

Scan

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

At JPCERT/CC, the following are classified as **scans**.

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

DoS/DDoS

DoS/DDoS refers to attacks against network resources such as servers and PCs on a network, and devices and lines that constitute the network, to render services unavailable.

At JPCERT/CC, the following are classified as **DoS/DDoS**.

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

Control System-related Incidents

Control system-related incidents refers to incidents related to control systems and various plants.

At JPCERT/CC, the following are classified as **control system-related incidents**.

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

Targeted Attack

Targeted attack refers to an attack that targets specific organizations, companies, industries, etc., attempting malware infection or information theft.

At JPCERT/CC, the following are classified as **targeted attacks**.

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

Other

Other refers to incidents not covered above.

Examples of items JPCERT/CC classifies as **other** are listed below.

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

When quoting or reprinting this document, please contact JPCERT/CC Public Relations (pr@jpcert.or.jp) for confirmation.

Company names and product names described in this document are trademarks or registered trademarks of their respective owners.

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

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

JPCERT/CC Quarterly Report [April 1, 2026 to June 30, 2026]

- Revision History
 - July 16, 2026 First Japanese version
 - September 18, 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/>