JPCERT/CC Incident Handling Report

October 1, 2023 - December 31, 2023

JPCERT Coordination Center

January 18, 2024

JPCERT CC®

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, 2023 through December 31, 2023, 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

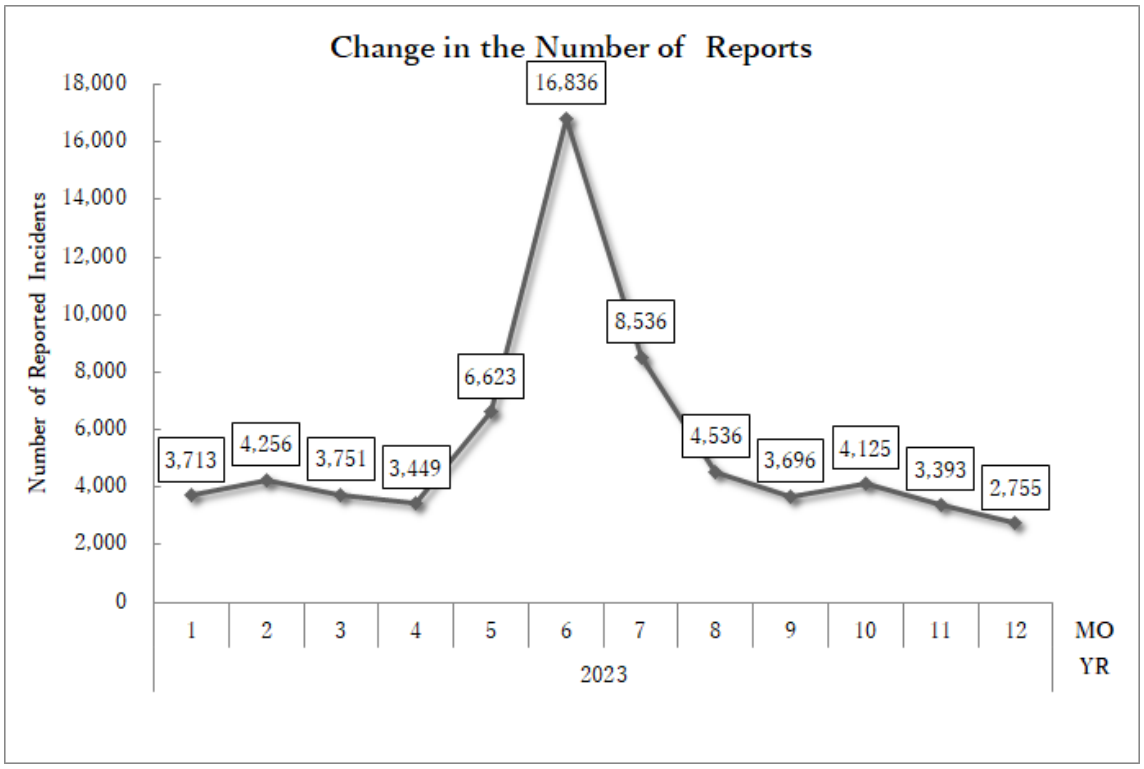
[Chart 1]shows the total number of incident reports, reported incidents and incidents that JPCERT/CC coordinated during this quarter.

[Chart 1: Number of incident reports]

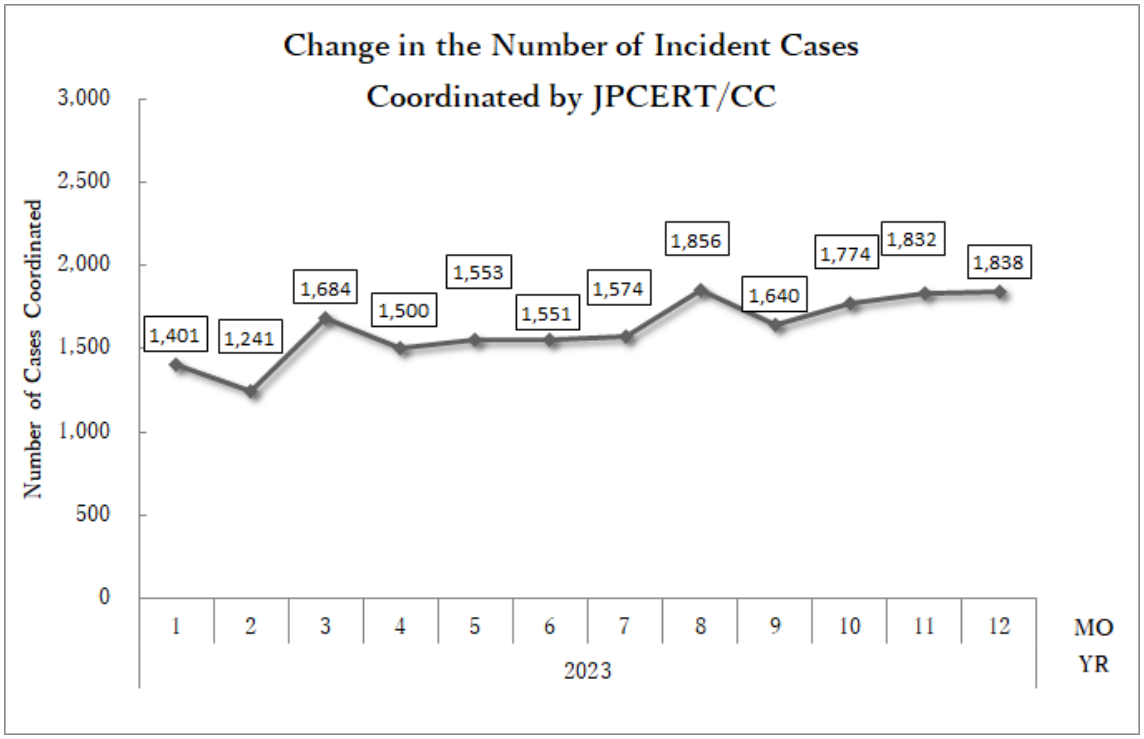
	Oct	Nov	Dec	Total	Last Qtr. Total
Number of Reports [(2)]	4,125	3,393	2,755	10,273	16,768
Number of Incident [(3)]	2,386	2,164	1,898	6,448	5,903
Cases Coordinated [(4)]	1,774	1,832	1,838	5,444	5,070

(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.

The total number of reports received in this quarter was 10,273. Of these, the number of cases that JPCERT/CC coordinated was 5,444. When compared with the previous quarter, the number of reports decreased by 39%, and the number of cases coordinated increased by 7%. Year on year, the number of reports decreased by 13.8%, and the number of cases coordinated decreased by 5%.
[Figure 1] and [Figure 2] show the monthly changes in the total number of reports and incident cases coordinated by JPCERT/CC over the past fiscal year.



[Figure 1: Change in the number of incident reports]

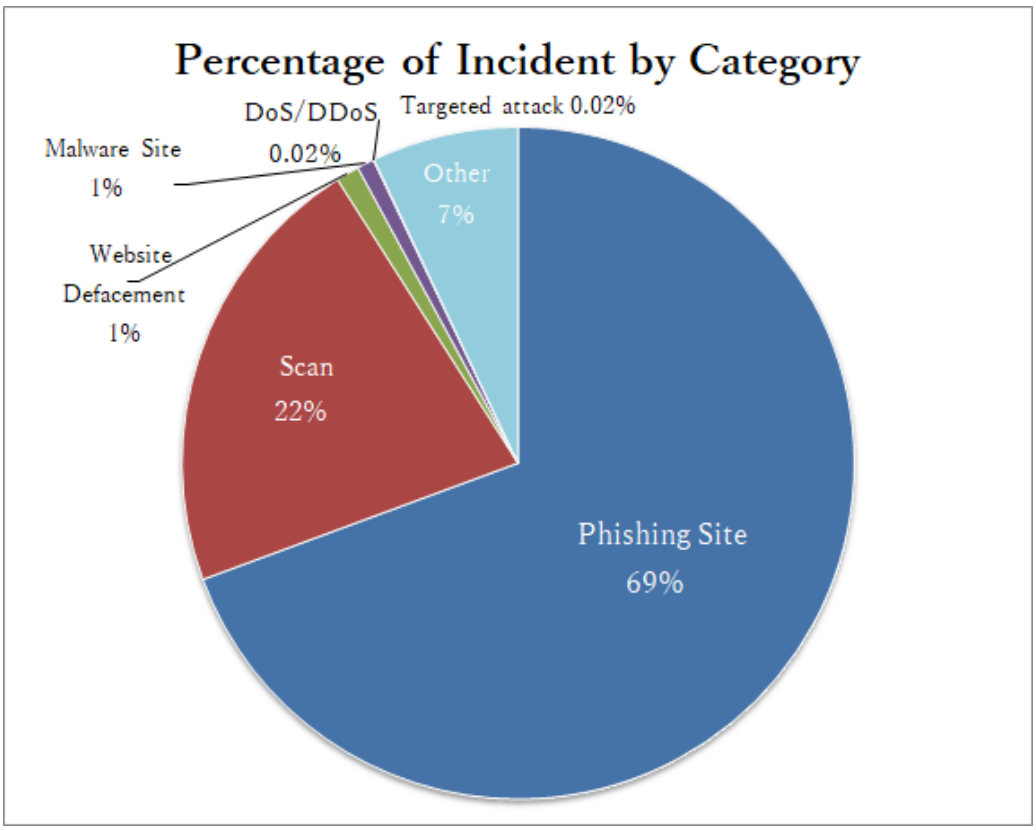


[Figure 2: Change in the number of incident cases coordinated]

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] shows a breakdown of the number of incidents reported during the quarter by category. A breakdown of the percentage is shown in[Figure 3].

[Chart 2: Number of incidents by category]

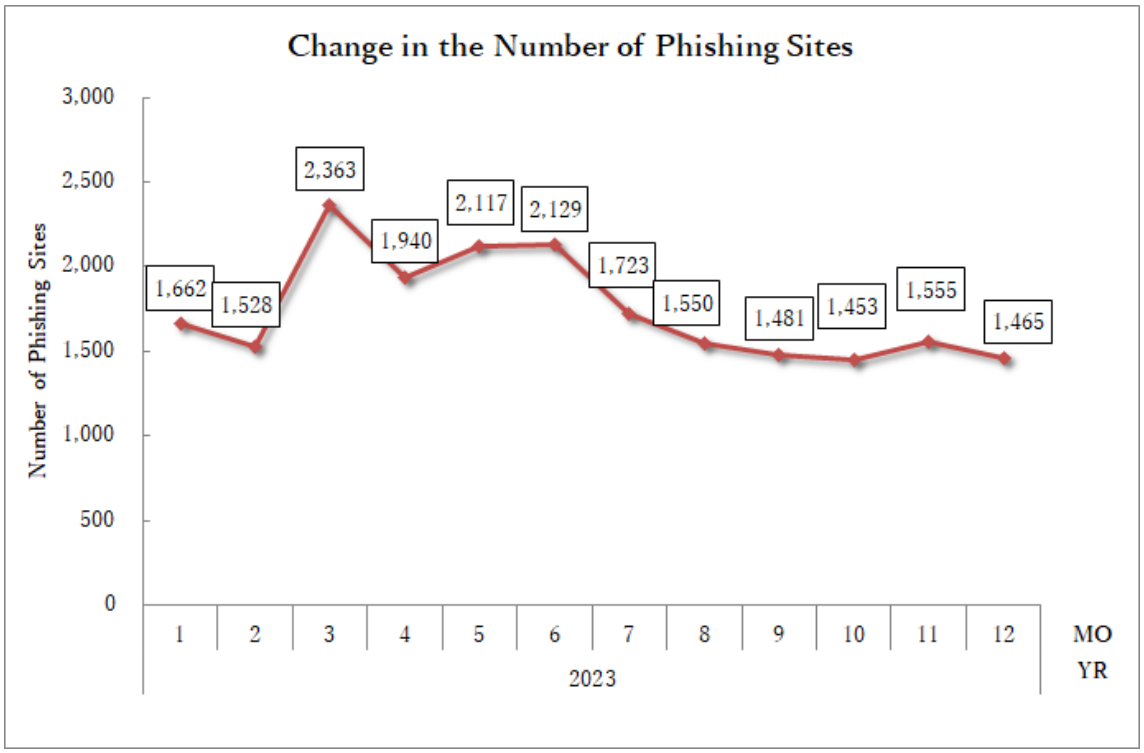
Incident Category	Oct	Nov	Dec	Total	Last Qtr. Total
Phishing Site	1,453	1,555	1,465	4,473	4,754
Website Defacement	44	15	13	72	124
Malware Site	19	19	15	53	89
Scan	735	348	310	1,393	639
DoS/DDoS	1	0	0	1	3
ICS Related	0	0	0	0	0
Targeted attack	0	0	1	1	2
Other	134	227	94	455	292



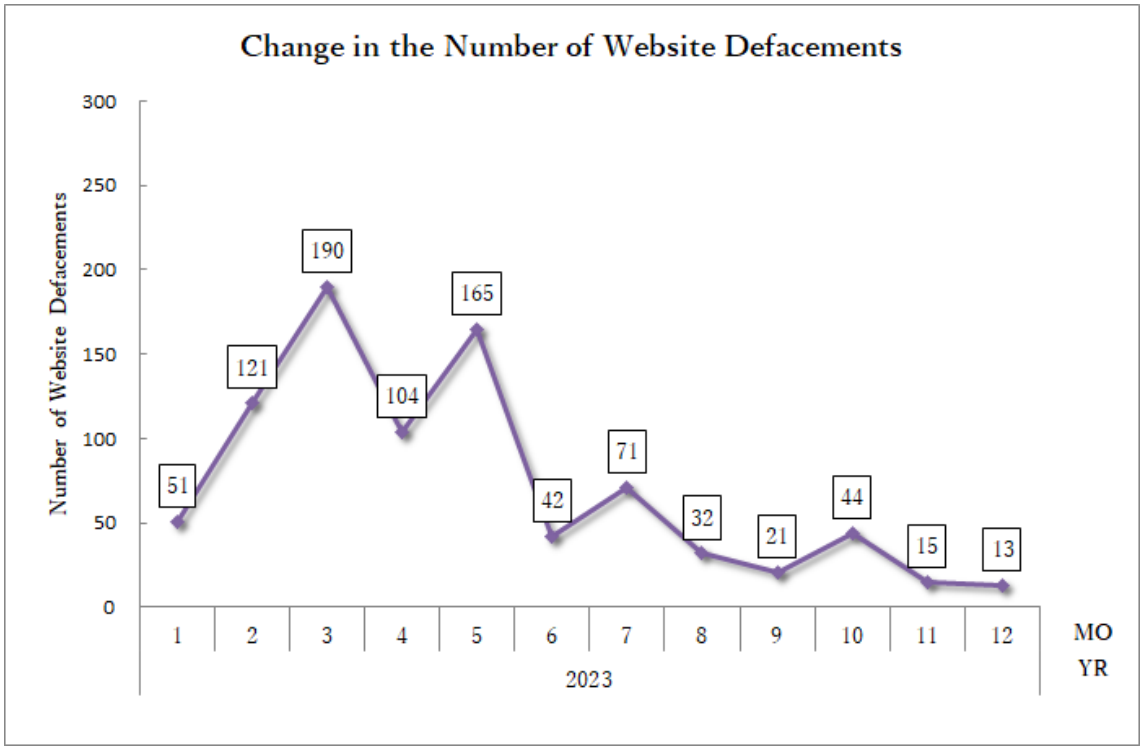
[Figure 3: Percentage of incidents by category]

Incidents categorized as phishing sites accounted for 69%, and those categorized as scans, which search for vulnerabilities in systems, made up 22%.

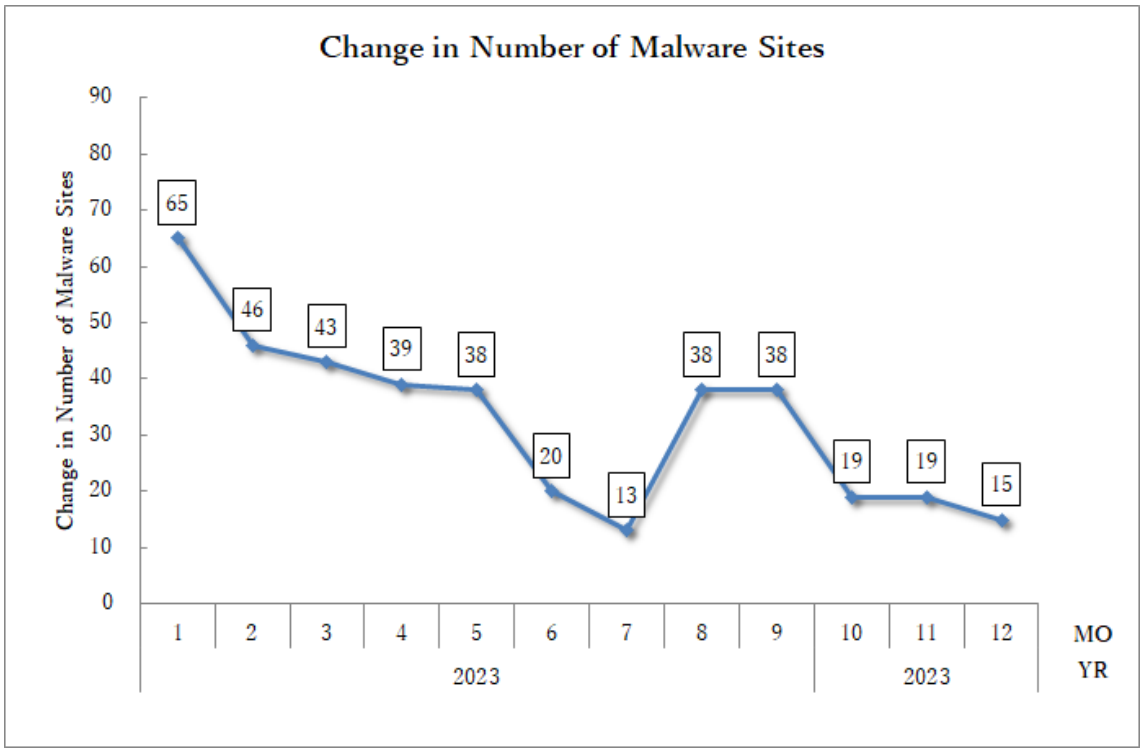
[Figure 4] through [Figure 7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



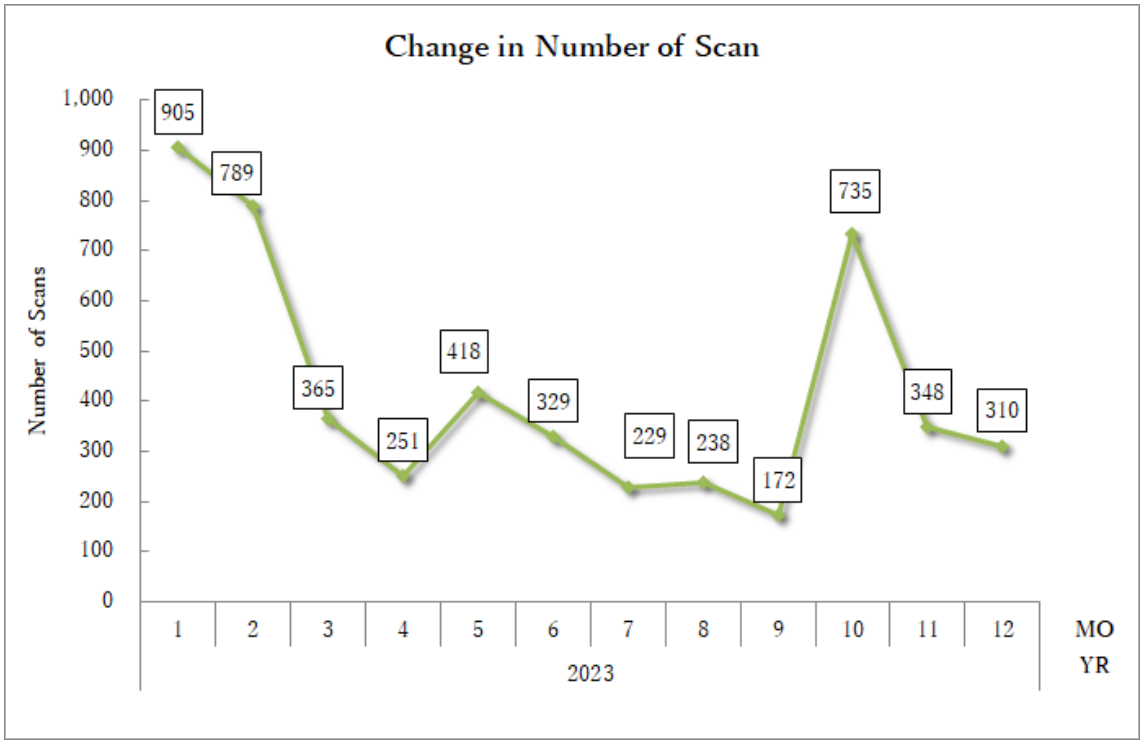
[Figure 4: Change in the number of phishing sites]



[Figure 5: Change in the number of website defacements]

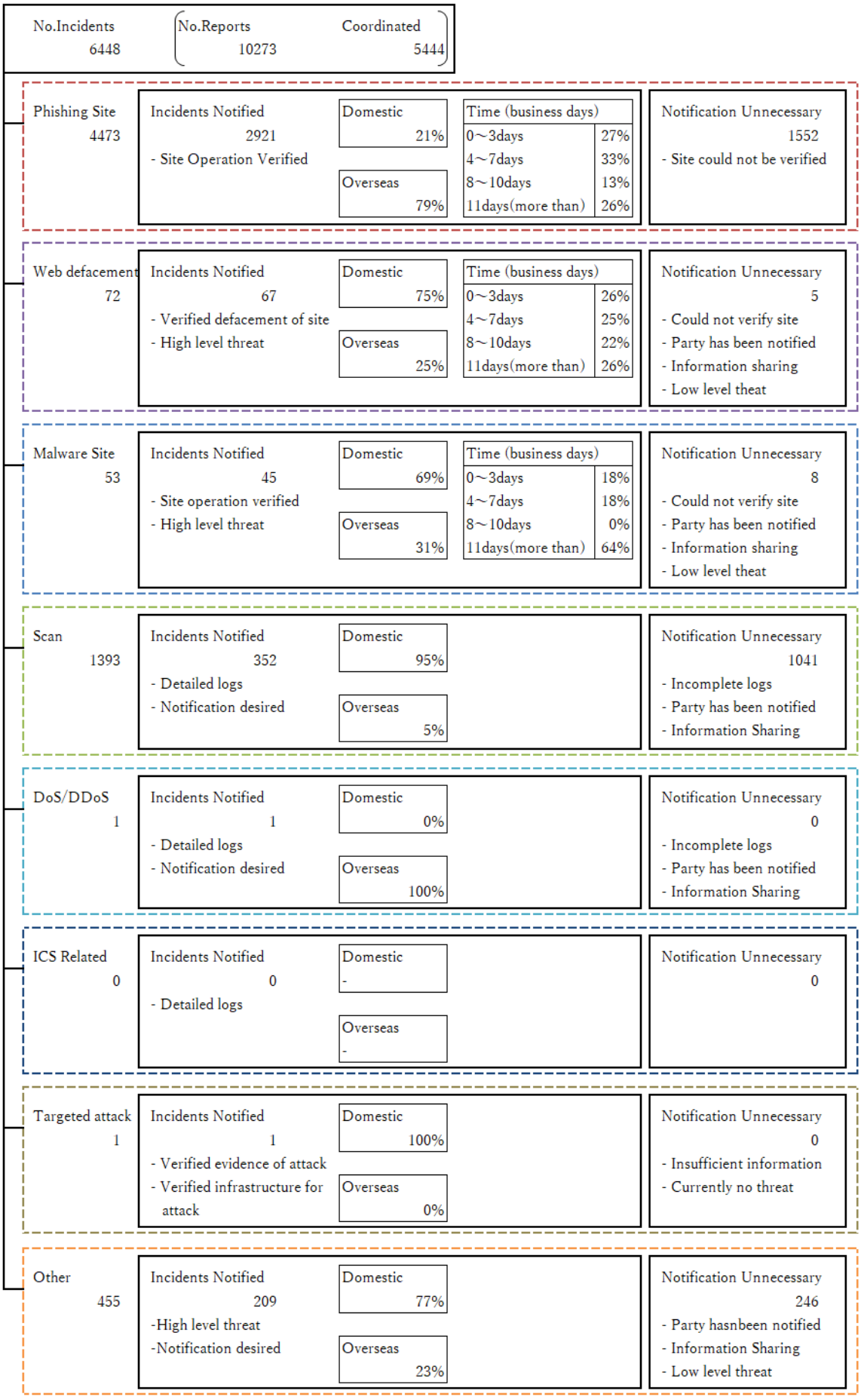


[Figure 6: Change in the number of malware sites]



[Figure 7: Change in the number of scans]

[Figure 8] provides an overview as well as a breakdown of the incidents that were coordinated /Handled.



[Figure 8: Breakdown of incidents coordinated/handled]

3. Incident Trends

3.1. Phishing Site Trends

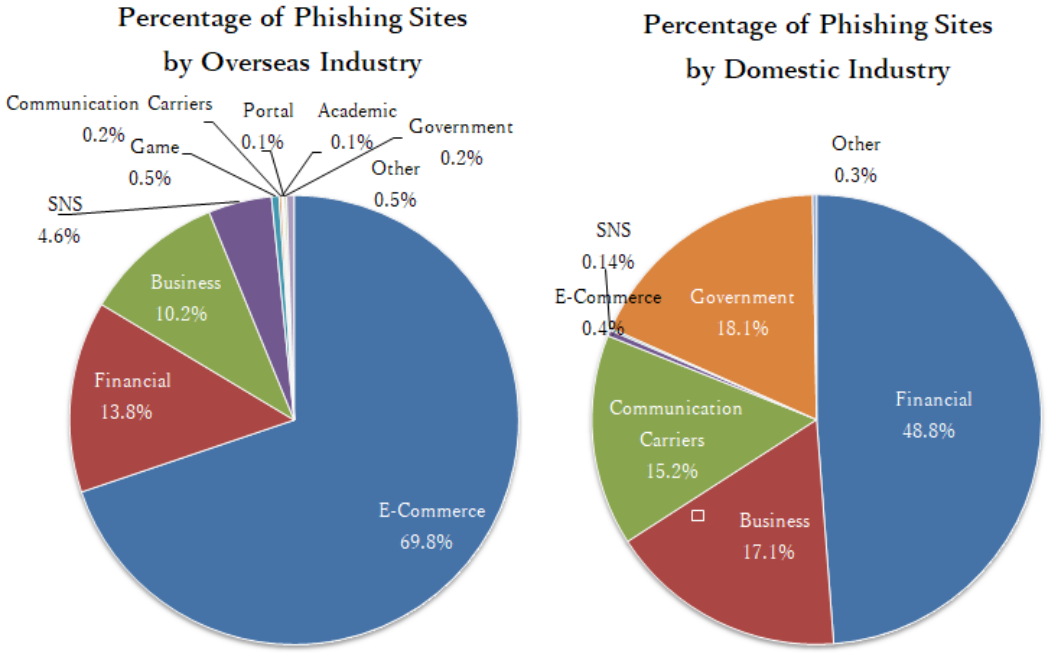
During this quarter, 4,473 reports on phishing sites were received, representing a 6% decrease from 4,754 in the previous quarter. This marks a 29% decrease from the same quarter last year (6,266).

During this quarter, there were 2,796 phishing sites that spoofed domestic brands, decreasing 8% from 3,029 in the previous quarter. There were 1,116 phishing sites that spoofed overseas brands, increasing 12% from 997 in the previous quarter. The numbers of brands that the phishing sites spoofed in this quarter are shown by brand type (domestic, overseas) in [Chart 3], and the percentages by industry for domestic and overseas brands are shown in [Figure 9].

[Chart 3: Number of reported phishing sites by domestic/overseas brand]

Phishing Site	Oct	Nov	Dec	Domestic/Overseas Total (%)
Domestic Brand	894	1,047	855	2,796 (63%)
Overseas Brand	371	278	467	1,116 (25%)
Unknown Brand (*5)	188	230	143	561 (13%)
Monthly Total	1,453	1,555	1,465	4,473

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



[Figure 9: Percentage of reported phishing sites by industry (domestic/overseas)]

Out of the total number of phishing sites reported to JPCERT/CC, 69.8% spoofed e-commerce websites for overseas brands and 48.8% spoofed financial websites for domestic brands, both representing the largest share respectively.

For overseas brands, phishing sites spoofing Amazon accounted for more than half of the phishing sites reported.
For domestic brands, phishing sites spoofing the Myna Points Project of the Ministry of Internal Affairs and Communications and Electronic Toll Collection (ETC) system usage inquiry services were reported in large numbers. Among domestic financial institutions, phishing sites spoofing EPOS Card, Aeon Card, and Sumitomo Mitsui Card continued to be seen in large numbers as in the previous quarter. Compared with the previous quarter, there were marked declines in the numbers of phishing sites spoofing Saison Card and PayPay.

The websites that JPCERT/CC coordinated with to take down phishing sites were 21% domestic and 79% overseas for this quarter, indicating a decrease in domestic parties compared to the previous quarter (domestic: 27%, overseas: 78%).

3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 72. This was a 42% decrease from 124 in the previous quarter.

During this quarter, JPCERT/CC confirmed a number of website defacement cases that involve redirecting the visitors to suspicious websites. Compromised websites were planted with a script as shown in [Figure 10], which was designed to redirect only first-time visitors to a suspicious website. The suspicious websites were confirmed to be lucky visitor scam sites and websites that exploit the browser's notification function.

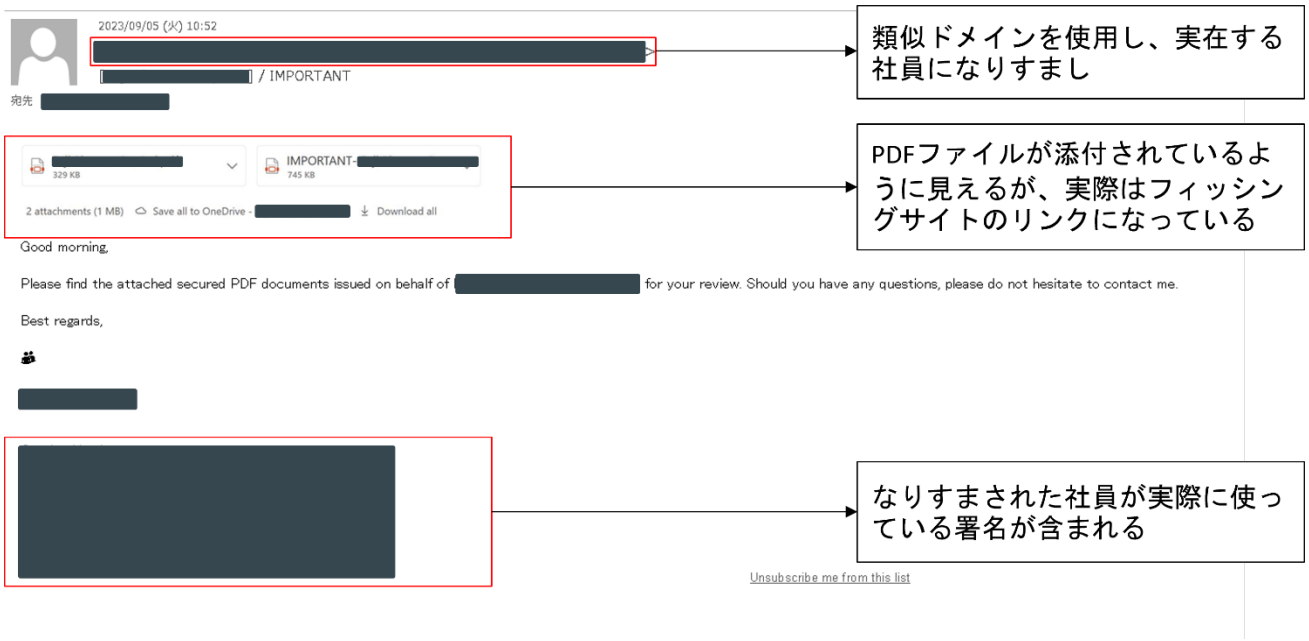
```
localStorage.setItem('test', 'testValue');

if ((localStorage.getItem('test') !== null) &&  (localStorage.getItem('click3') == null)){

    var click_r = false;
    document.addEventListener("click", function(){

    if(click_r == false){
    localStorage.setItem('click3', 'click3');
    window.open("[redacted]");
    click_r = true;
    }
    });
}
```

[Figure 10: Script for displaying a suspicious website]

3.3. Targeted Attack Trends

There was 1 incident categorized as a targeted attack.

This quarter, JPCERT/CC received a report of spoofed emails being sent to impersonate an organization. The attackers had obtained in advance a domain that looked confusingly similar to that of the organization they were trying to impersonate and used that domain to send emails using the name of an actual employee of that organization. As shown in [Figure 11], the text of the emails contained a signature that the impersonated employee actually uses. Moreover, these emails were targeted specifically to the business partners of the spoofed organization, instead of a large number of unspecified recipients, which suggests that the attackers may have stolen the email information of the related parties beforehand.



[Figure 11: Example of a spoofed email]

JPCERT/CC has confirmed that these attacks started around March 2022. A number of organizations other than the one reported this quarter have been subject to the attacks, and in all cases emails sent from a misleading domain ([Chart 4]) were found, with a text that contains a seemingly legitimate signature.

[Chart 4: Examples of misleading domains]

Legitimate domains	Domains that look confusingly similar to the legitimate domains
example[.]jp	example-jp[.]com
example[.]com	example[.]co
example[.]com	exmple[.]com

3.4. Other Incident Trends

The number of malware sites reported in this quarter was 53. This was a 40% decrease from 89 in the previous quarter.

The number of scans reported in this quarter was 1,393. This was a 118% increase from 639 in the previous quarter. The top 10 ports that the scans targeted are listed in [Chart 5]. Ports targeted frequently were SSH (22/TCP), Telnet (23/TCP), SMTP (25/TCP) and HTTP (80/TCP).

[Chart 5: Top 10 ports by number of scans]

Port	Oct	Nov	Dec	Total
22/tcp	604	257	172	1,033
23/tcp	79	70	77	226
25/tcp	1	4	38	43
80/tcp	12	5	2	19
445/tcp	9	5	3	17
443/tcp	7	1	7	15
8080/tcp	5	3	3	11
56575/tcp	10	0	1	11
37215/tcp	1	0	4	5
143/tcp	0	3	2	5

There were 455 incidents categorized as other. This was a 56% increase from 292 in the previous quarter.

4. Incident Handling Case Examples

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

(1) Coordination involving a vulnerability (CVE-2023-45727) in Proself

On October 10, 2023, North Grid announced that an XML external entity (XXE) vulnerability was found in Proself, an online storage-building package product. After confirming attacks exploiting this vulnerability to send files in a system to external destinations, JPCERT/CC also issued a security alert on October 10.

Security alert concerning an attack exploiting an XML external entity (XXE) vulnerability in Proself (Japanese only)
https://www.jpcert.or.jp/at/2023/at230022.html

JPCERT/CC notified system administrators in Japan who use versions of Proself that appear to be unpatched. Users of the affected products are advised to take appropriate steps quickly. Since attacks may have already been carried out, users are encouraged to see if there has been any suspicious communication, referring to the indicator information published by JPCERT/CC as a reference.

Security alert concerning targeted cyber attack campaigns aimed at Internet-facing IT assets of Japanese organizations (Japanese only)
https://www.jpcert.or.jp/at/2023/at230029.html

(2) Coordination involving a vulnerability (CVE-2023-20198) in Cisco IOS XE

On October 16, 2023, Cisco announced a privilege escalation vulnerability in a web UI feature of its Cisco IOS XE software. JPCERT/CC released a security alert as well on October 18 since this vulnerability may be exploited by unauthenticated third parties to remotely create a highest-privilege account and control the system.

Security alert concerning a web UI vulnerability (CVE-2023-20198) in Cisco IOS XE (Japanese only)
https://www.jpcert.or.jp/at/2023/at230025.html

JPCERT/CC has received reports of this vulnerability being exploited to create a backdoor from organizations in Japan and abroad. JPCERT/CC has notified the administrators of devices in Japan suspected of such backdoor installation. Users of the affected products are advised to update it as soon as possible.

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.)

These activities are sponsored by the Ministry of Economy, Trade and Industry as part of the "Coordination Activities for International Cooperation in Responding to Cyber Attacks for the 2023.