JPCERT CC®

JPCERT Coordination Center

デジタル署名者 : JPCERT Coordination Center
DN : c=JP, st=Tokyo, l=Chuo-ku, serialNumber=AATL20231109322437, o=JPCERT Coordination Center, cn=JPCERT Coordination Center, email=office@jpcert.or.jp
日付 : 2024.05.31 14:36:23 +09'00'

JPCERT/CC Incident Handling Report

January 1, 2024 - March 31, 2024

JPCERT Coordination Center

April 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 January 1, 2024 through March 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 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]

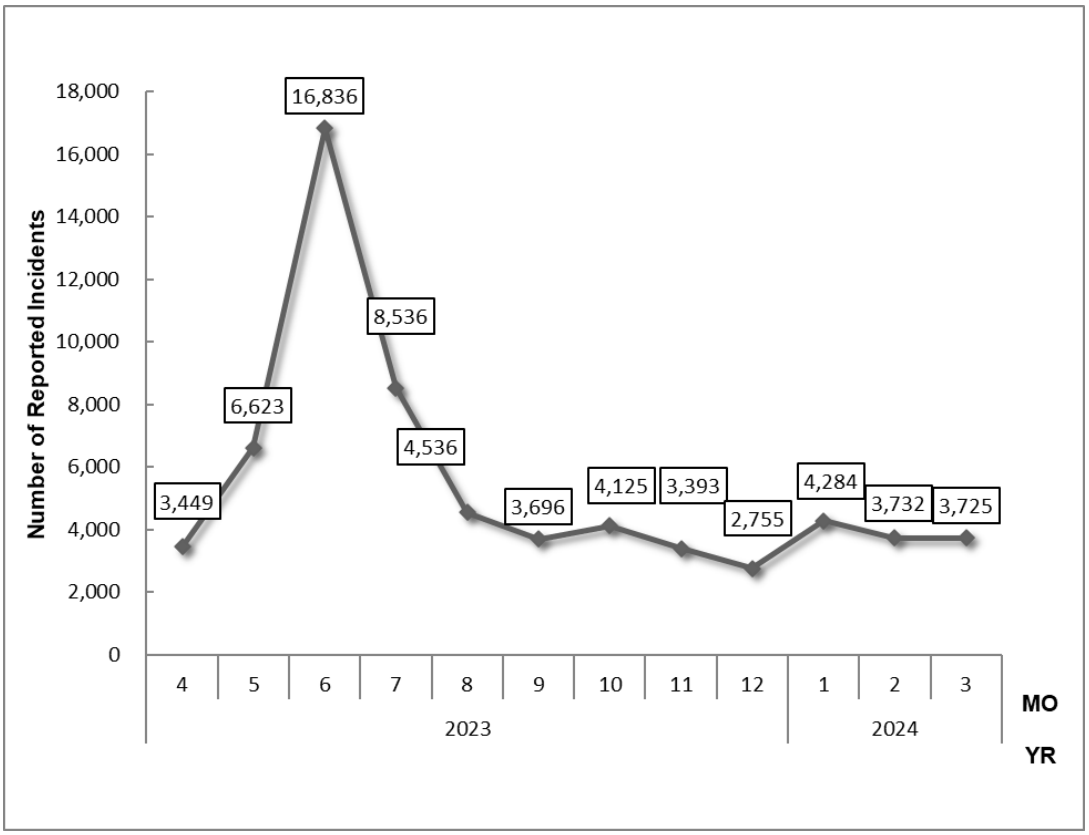
	Jan	Feb	Mar	Total	Last Qtr. Total
Number of Reports [(2)]	4,284	3,732	3,725	11,741	10,273
Number of Incident [(3)]	1,988	1,956	2,145	6,089	6,448
Cases Coordinated [(4)]	1,719	1,596	1,287	4,602	5,444

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

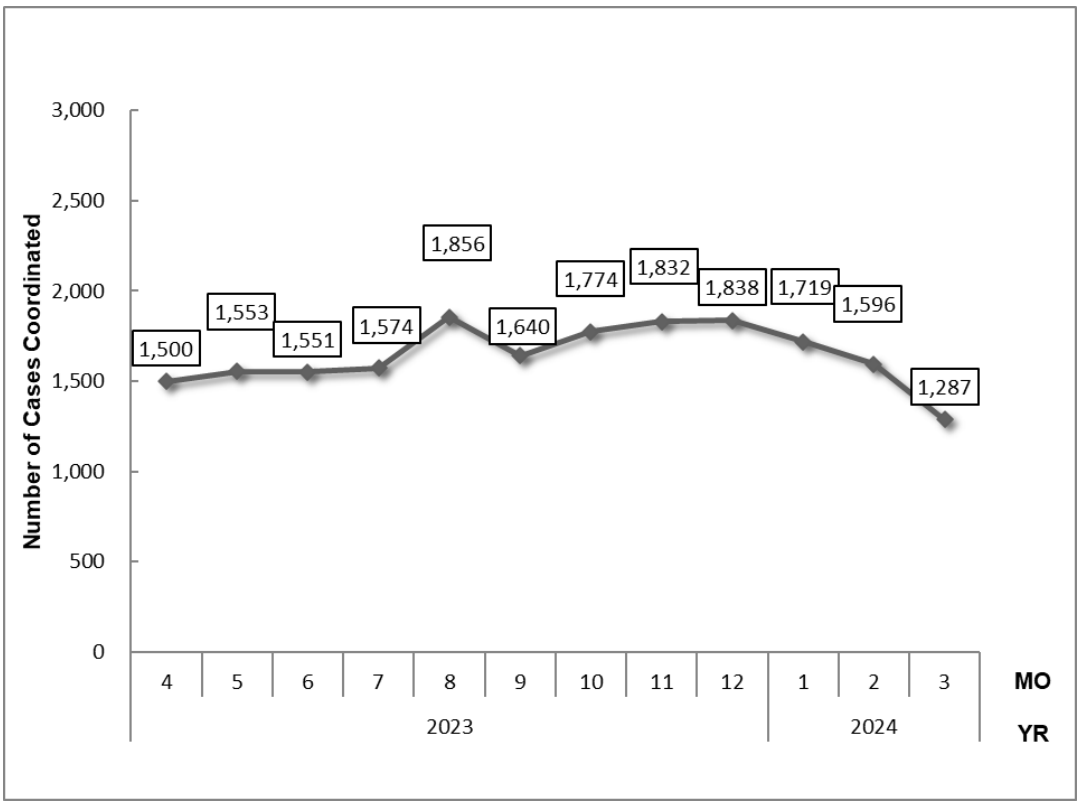
(3) "Number of Incidents" refers to the number of incidents contained in each report. Multiple reports on the same incidents are counted as 1 incident.

(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 11,741. Of these, the number of cases that JPCERT/CC coordinated was 4,602. When compared with the previous quarter, the number of reports increased by 14%, and the number of cases coordinated decreased by 15%. Year on year, the number of reports increased by 0.2%, and the number of cases coordinated increased by 6%.
[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]

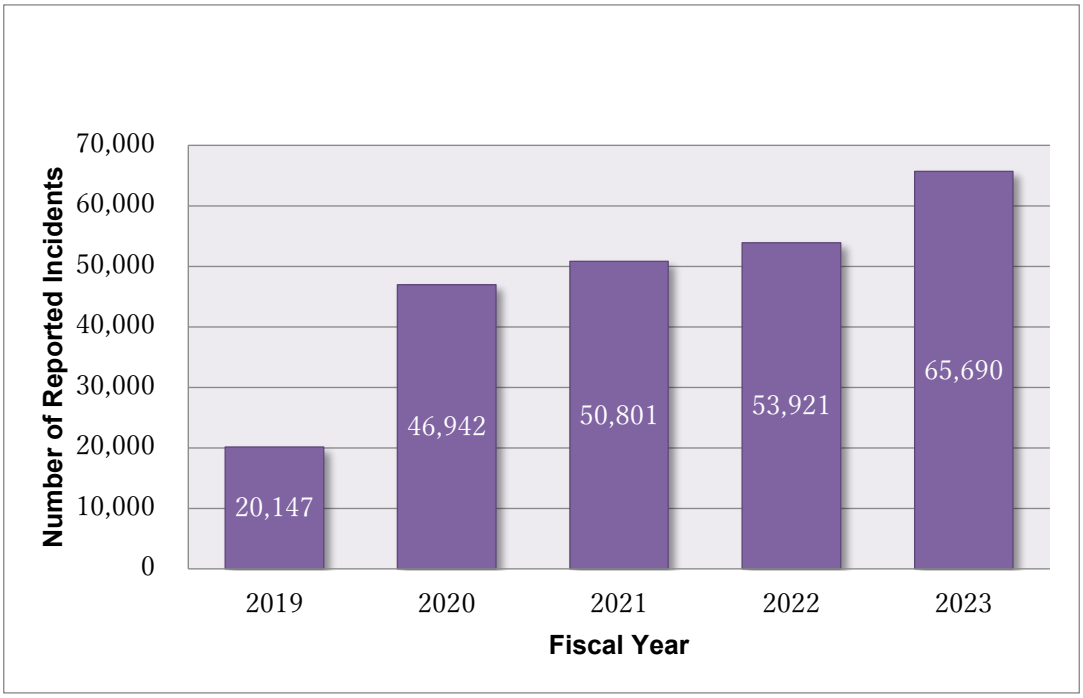
[Reference] Statistical Information by Fiscal Year

[Chart 2] shows the number of reports in each fiscal year over the past 5 years including FY2023. Each fiscal year begins on April 1 and ends on March 31 of the following year.

[Chart 2: Change in the total number of reports]

FY	2019	2020	2021	2022	2023
Number of Reports	20,147	46,942	50,801	53,921	65,690

The total number of reports received in FY2023 was 65,690, increasing 22% year on year from 53,921. [Figure 3] shows the change in the total number of cases coordinated in the past 5 years.



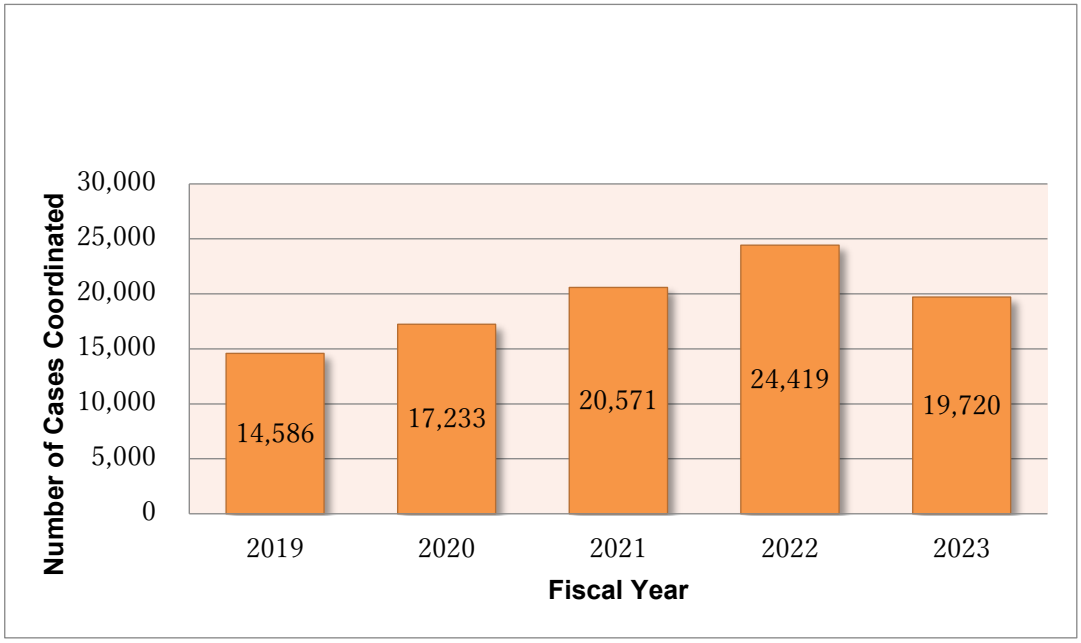
[Figure 3: Change in the total number of reports (by fiscal year)]

[Chart 3] shows the number of cases coordinated in each fiscal year over the past 5 years including FY2023.

[Chart 3: Change in the number of reports and cases coordinated]

FY	2019	2020	2021	2022	2023
Number of Cases Coordinated	14,586	17,233	20,571	24,419	19,720

The total number of cases coordinated in FY2023 was 19,720, decreasing 19% year on year from 24,419. [Figure 4] shows the change in the total number of cases coordinated in the past 5 years.

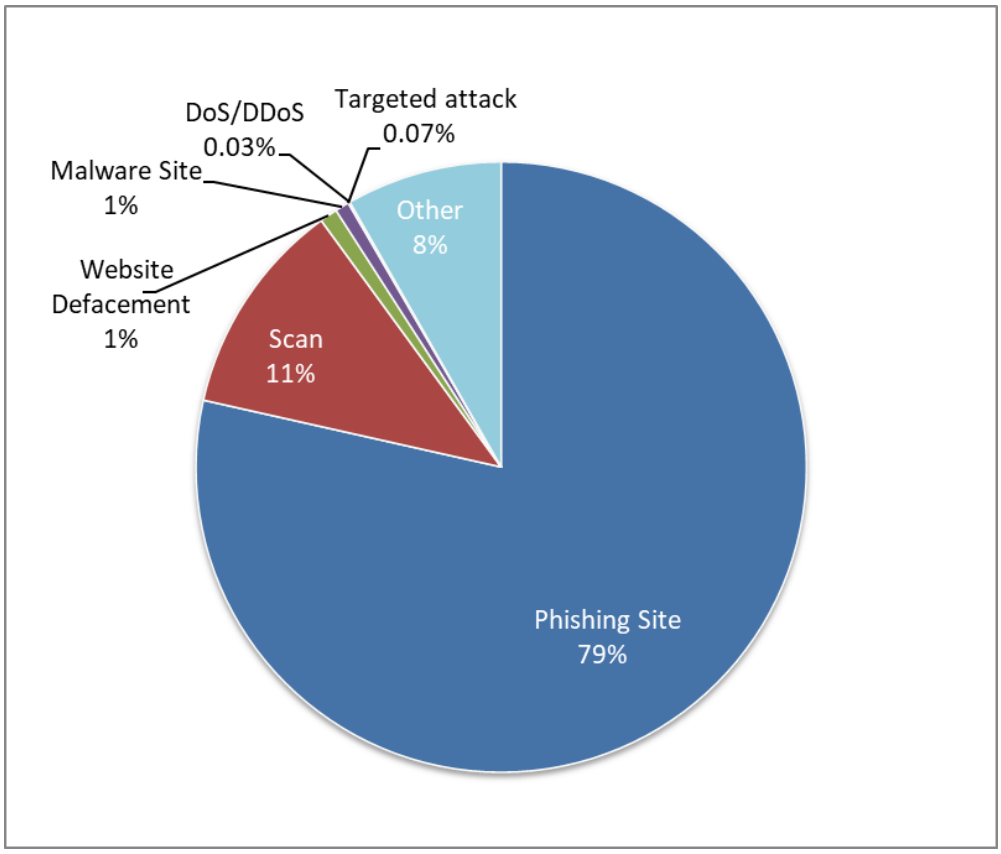


[Figure 4: Change in the total number of cases coordinated (by fiscal year)]

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

[Chart 4: Number of incident reports by category]

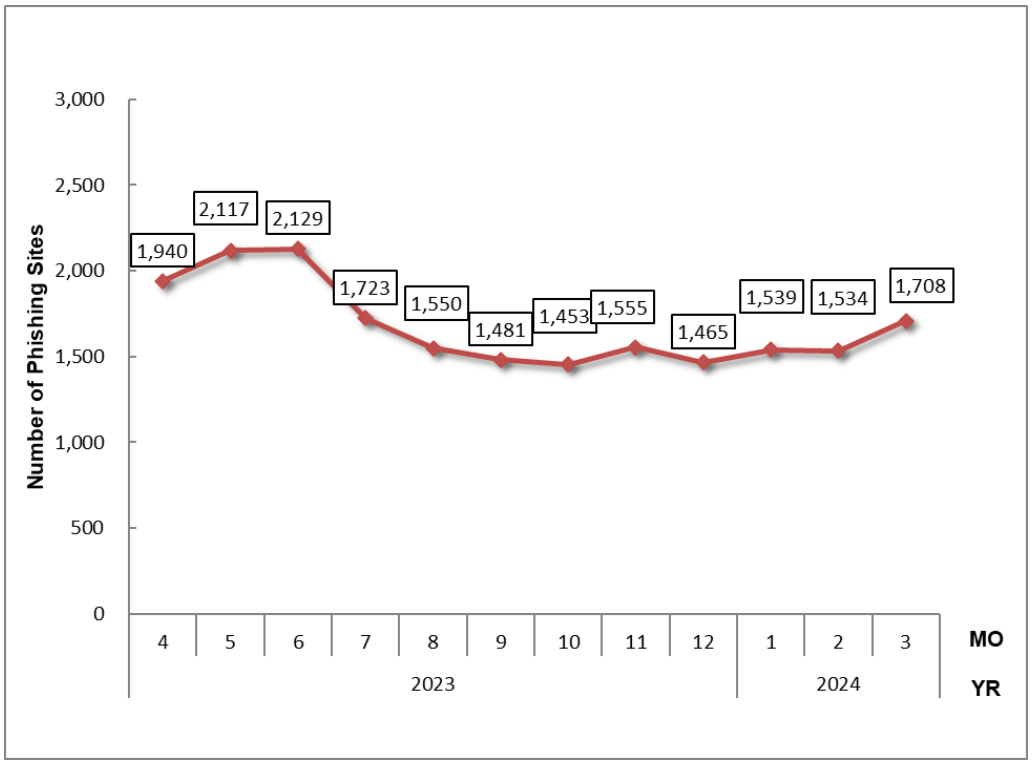
Incident Category	Jan	Feb	Mar	Total	Last Qtr. Total
Phishing Site	1,539	1,534	1,708	4,781	4,473
Website Defacement	20	18	19	57	72
Malware Site	11	14	20	45	53
Scan	280	240	177	697	1,393
DoS/DDoS	0	1	1	2	1
ICS Related	0	0	0	0	0
Targeted attack	2	0	2	4	1
Other	136	149	218	503	455



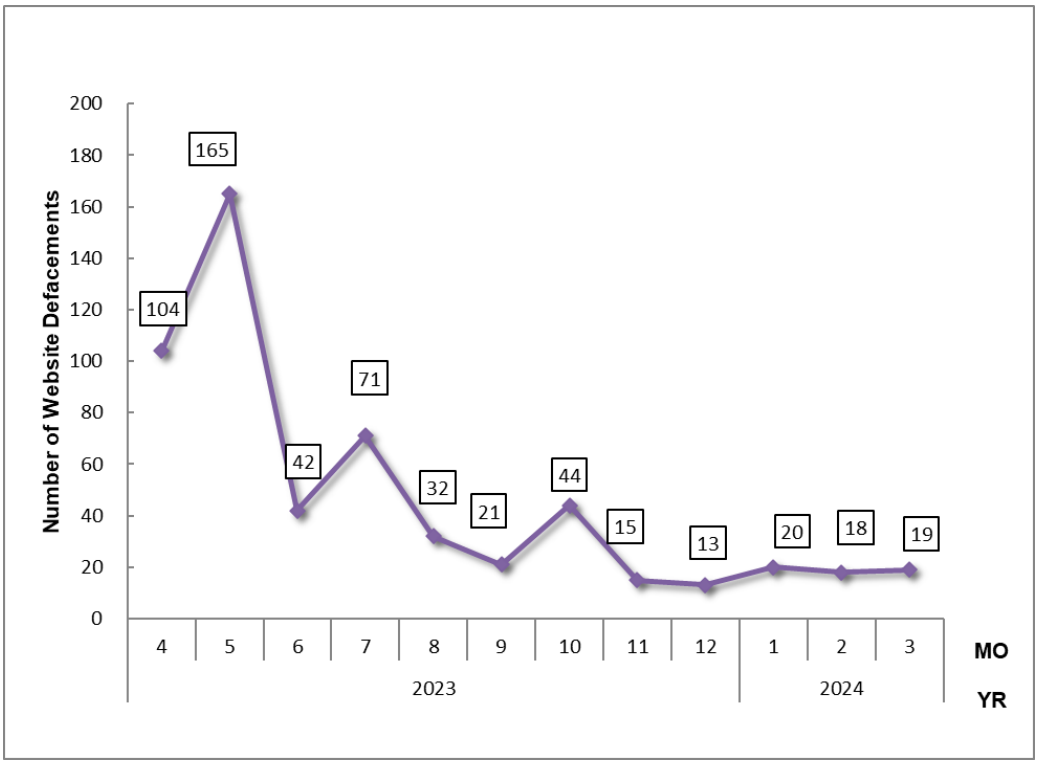
[Figure 5: Percentage of incidents by category]

Incidents categorized as phishing sites accounted for 79%, and those categorized as scans, which search for vulnerabilities in systems, made up 11%.

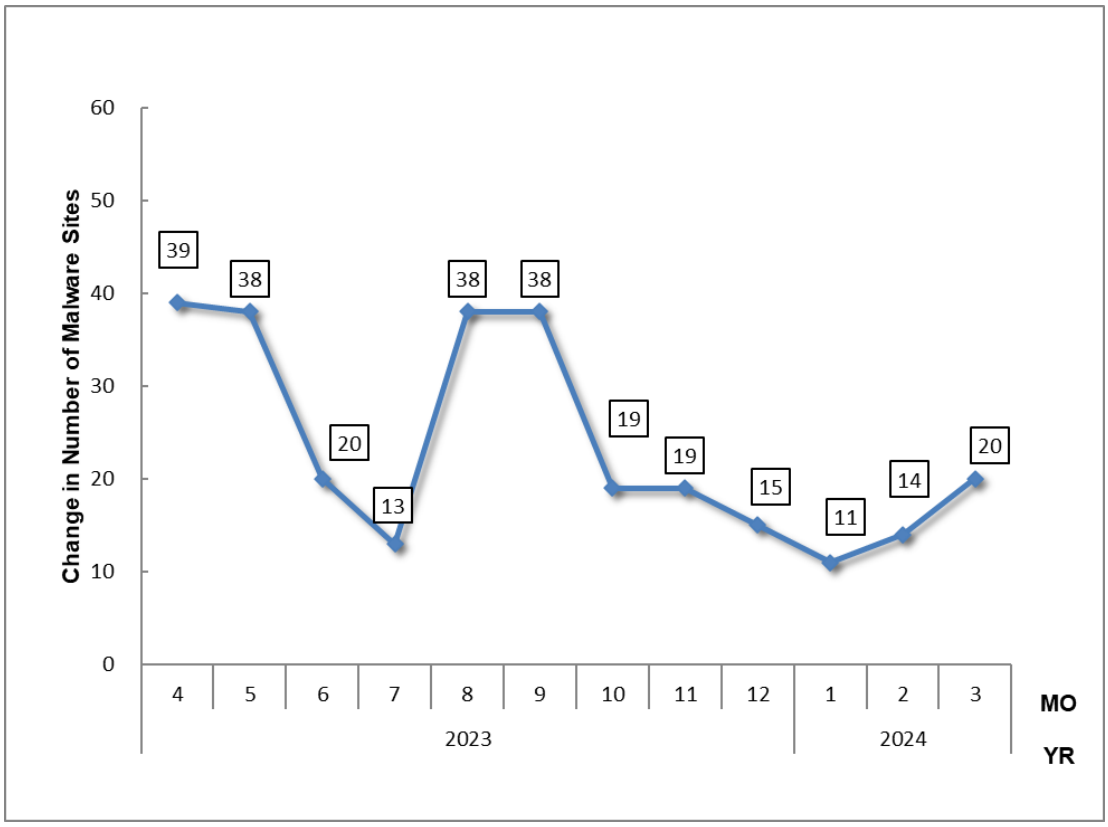
[Figure] through [Figure] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



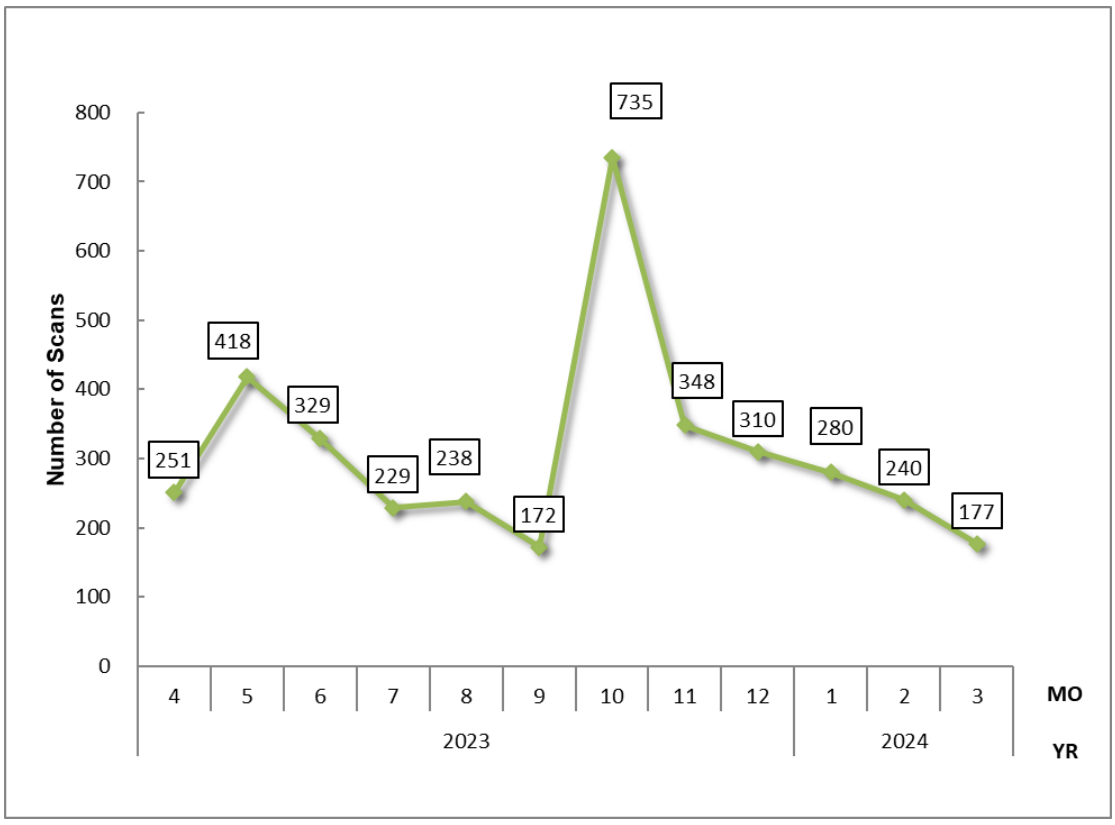
[Figure 6: Change in the number of phishing sites]



[Figure 7: Change in the number of website defacements]

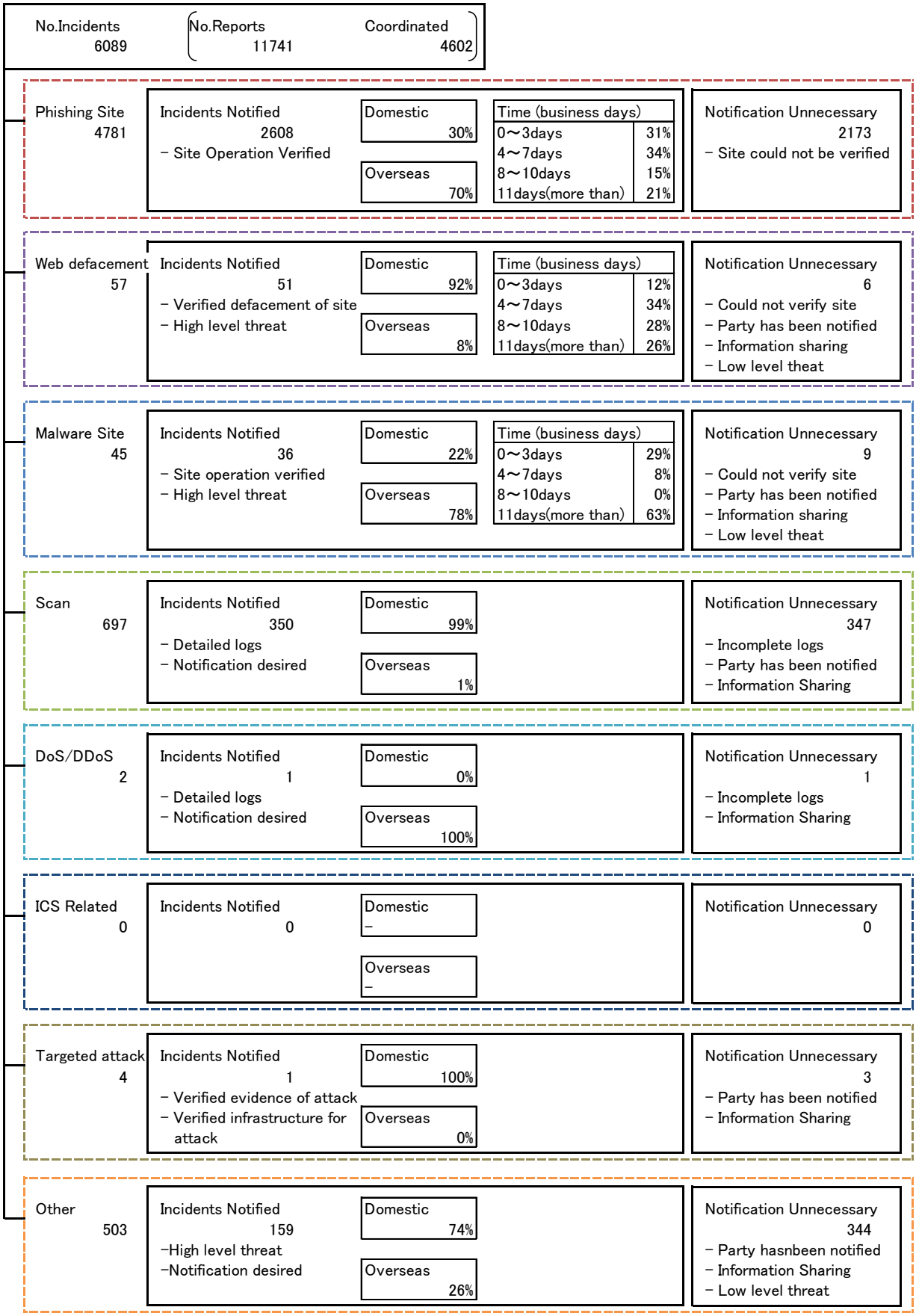


[Figure 8: Change in the number of malware sites]



[Figure 9: Change in the number of scans]

[Figure 10] provides an overview as well as a breakdown of the incidents that were coordinated /Handled.



[Figure 10: Breakdown of incidents coordinated/handled]

3. Incident Trends

3.1. Phishing Site Trends

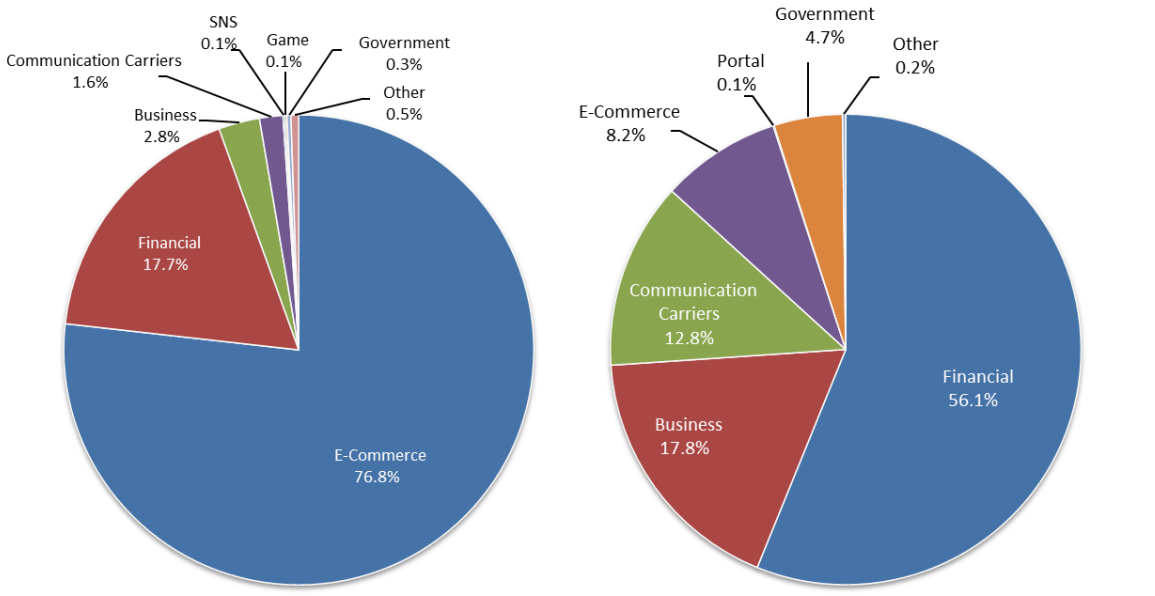
During this quarter, 4,781 reports on phishing sites were received, representing a 7% increase from 4,473 in the previous quarter. This marks a 14% decrease from the same quarter last year (5,553).

During this quarter, there were 3,226 phishing sites that spoofed domestic brands, increasing 15% from 2,796 in the previous quarter. There were 745 phishing sites that spoofed overseas brands, decreasing 33% from 1,116 in the previous quarter. The numbers of phishing sites reported in this quarter for domestic and overseas brands are shown in [Chart 5]. The percentages of phishing sites reported in this quarter by industry for domestic and overseas brands are shown in [Figure 11].

[Chart 5: Number of phishing sites for domestic and overseas brands]

Phishing Site	Jan	Feb	Mar	Domestic/Overseas Total (%)
Domestic Brand	1,076	1,134	1,016	3,226 (67%)
Overseas Brand	220	145	380	745 (16%)
Unknown Brand (5)	243	255	312	810 (17%)
Monthly Total	1,539	1,534	1,708	4,781

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



[Figure 11: Percentage of reported phishing sites by industry for domestic (Right) and overseas brands (Left)]

Out of the total number of phishing sites reported to JPCERT/CC, 76.8% spoofed e-commerce websites for overseas brands and 56.1% 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 Eki-Net 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.

The websites that JPCERT/CC coordinated with to take down phishing sites were 30% domestic and 70% overseas for this quarter, indicating an increase in domestic parties compared to the previous quarter (domestic: 21%, overseas: 79%).

3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 57. This was a 21% decrease from 72 in the previous quarter.

During this quarter, JPCERT/CC confirmed a number of cases in which compromised websites redirected users who accessed the website to a fake e-commerce site. Compromised websites were planted with a script like the one shown in [Figure 12], which redirects users to suspicious websites based on the JavaScript settings of the web browser used.

```
<html lang="jp">
<head>
    <meta content="text/html; charset=utf-8" http-equiv="Content-Type" />
    <meta http-equiv="refresh" content="0; url=https://[redacted]" />
</head>
<body>
  <noscript>
    <meta http-equiv="refresh" content="0; url=https://[redacted]" />
  </noscript>
  <script>
    document.location.href = "https://[redacted]";
  </script>
```

[Figure 12 : Script for displaying a suspicious website]

3.3. Targeted Attack Trends

There were 4 incidents categorized as a targeted attack.

This quarter, JPCERT/CC received a number of reports of targeted attacks using malware dubbed NOOPDOOR. It is suspected that VPN vulnerabilities and other security holes may have been exploited

as initial entry points. After infiltrating the network, the attackers placed NOOPDOOR on a number of devices. Another characteristic of these attacks is that the attackers have eventually removed the malware that they had placed.

3.4. Other Incident Trends

The number of malware sites reported in this quarter was 45. This was a 15% decrease from 53 in the previous quarter.

The number of scans reported in this quarter was 697. This was a 50% decrease from 1,393 in the previous quarter. The top 10 ports that the scans targeted are listed in [Chart]. Ports targeted frequently were SSH (22/TCP), Telnet (23/TCP), SMTP (25/TCP) and HTTP (80/TCP).

[Chart 6: Top 10 ports by number of scans]

Port	Jan	Feb	Mar	Total
22/tcp	107	118	68	293
23/tcp	106	78	80	264
25/tcp	36	23	17	76
80/tcp	14	10	8	32
37215/tcp	9	3	1	13
5888/tcp	5	2	0	7
445/tcp	2	2	0	4
2323/tcp	2	1	1	4
143/tcp	1	2	1	4
443/tcp	1	1	1	3

There were 503 incidents categorized as other. This was a 11% increase from 455 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 vulnerabilities in Ivanti Connect Secure

On January 10, 2024, Ivanti announced that vulnerabilities were found in Ivanti Connect Secure (formerly Pulse Connect Secure) and Ivanti Policy Secure gateways. The reported vulnerabilities include an authentication bypass vulnerability (CVE-2023-46805) and a command injection vulnerability (CVE-2024-21887), which can be exploited by a third party to remotely execute any commands. As the exploitation of these vulnerabilities were already confirmed, JPCERT/CC also issued a security alert on January 11. Subsequently, Ivanti further reported several related vulnerabilities. These included a privilege escalation vulnerability (CVE-2024-21888), SSRF vulnerability (CVE-2024-21893), and XML external entity (XXE) vulnerability (CVE-2024-22024). Accordingly, JPCERT/CC released a document outlining countermeasures and exploitation cases on February 21.

Security alert concerning Ivanti Connect Secure and Ivanti Policy Secure vulnerabilities (CVE-2023-46805 and CVE-2024-21887) (Japanese only)
https://www.jpcert.or.jp/at/2024/at240002.html

Status of Ivanti Connect Secure and other vulnerabilities since January 2024 (Japanese only)
https://www.jpcert.or.jp/newsflash/2024021601.html

Based on information provided by external organizations, JPCERT/CC alerted system administrators in Japan who were using devices suspected of being planted with a webshell or backdoor, or devices with unpatched vulnerabilities and a risk of being hacked.
Furthermore, JPCERT/CC has been consulted by a number of organizations that suffered damage due to these vulnerabilities and has confirmed a number of cases in which WIREFIRE webshell or ZIPLINE backdoor has been placed since January 11, immediately after the vulnerabilities were disclosed. Since January 16, when proof-of-concept (PoC) exploits attacking these vulnerabilities were released, attacks that plant devices with a cryptocurrency mining tool have also been confirmed. Some organizations reported that their internal integrity checker for Ivanti products were altered so that the planted webshell and backdoor could not be detected.

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.

If you would like to quote or reprint this document, please contact the Public Relations of JPCERT/CC (pr@jpcert.or.jp). For the latest information, please refer to JPCERT/CC's website.

JPCERT Coordination Center (JPCERT/CC)
https://www.jpcert.or.jp/english/

Company names and product names in this document are the trademarks or registered trademarks of the respective companies.