# JPCERT/CC Incident Handling Report

## January 1, 2022 ～ March 31, 2022

JPCERT Coordination Center
April 14, 2022

## 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 statistics and case examples for incident reports received during the period from January 1, 2022 through March 31, 2022.

[*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

[Chart1] 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] | 5,306 | 5,822 | 5,060 | 16,188 | 11,870 |
| Number of Incident [*3] | 3,083 | 2,890 | 3,396 | 9,369 | 9,807 |
| Cases Coordinated [*4] | 1,723 | 1,632 | 2,203 | 5,558 | 6,554 |

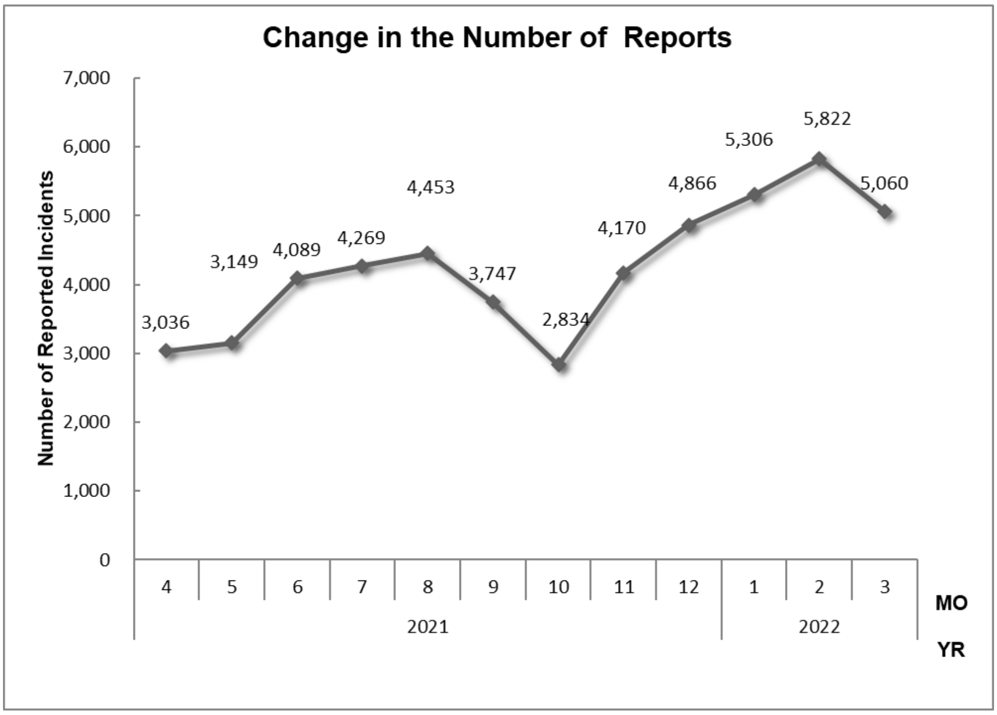
[*2] "Number of Reports" refers to the total number of reports sent through the web form, e-mail or FAX.

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

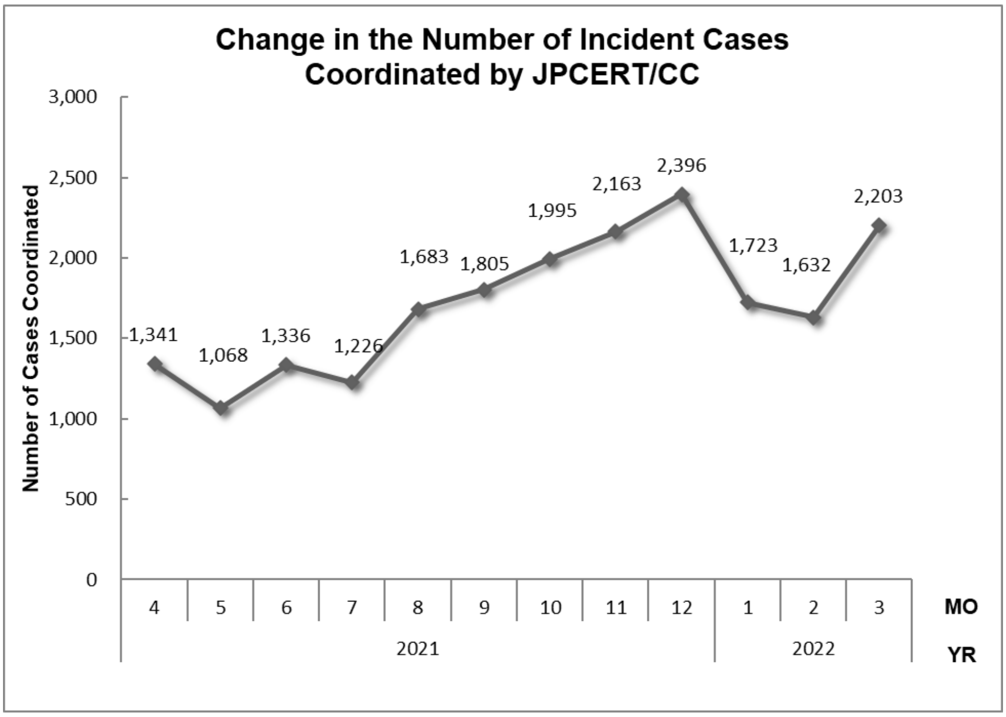
[*4] "Number of Cases Coordinated" refers to the number of cases where coordination took place to prevent the spreading of an incident by sending them a report and asking the site administrator to address any issues.

The total number of reports received in this quarter was 16,188. Of these, the number of domestic and overseas organizations that JPCERT/CC coordinated with was 5,558. When compared with the previous quarter, the total number of reports increased by 36%, and the number of cases coordinated decreased by 15%. Year on year, the number of reports increased by 68%, and the number of cases coordinated increased by 39%.

[Figure 1] and [Figure 2] show the monthly changes in the number of reports and incident cases coordinated by JPCERT/CC over the past year.



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



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

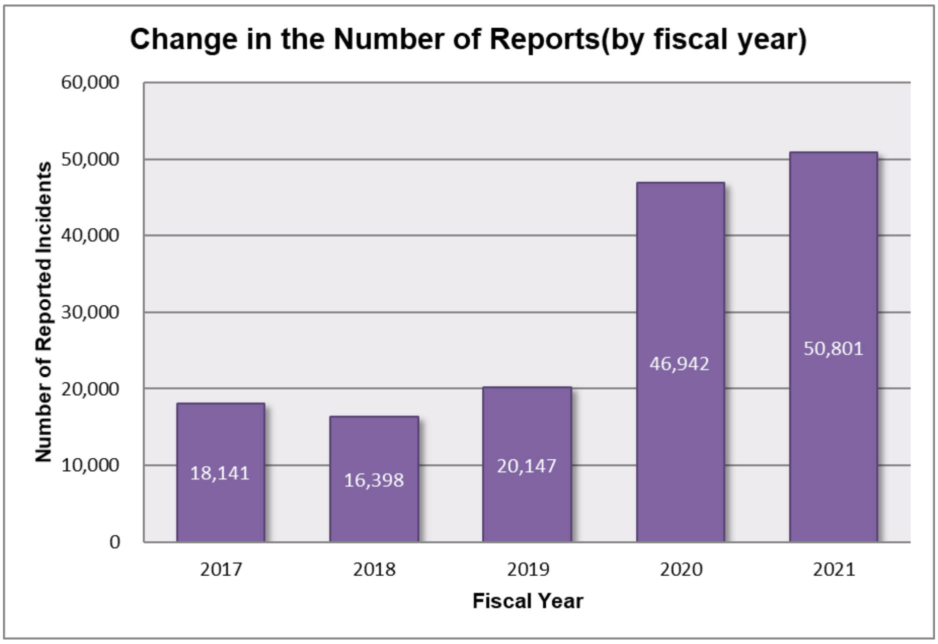
**[Reference] Statistical Information by Fiscal Year**

[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 | 2017 | 2018 | 2019 | 2020 | 2021 |
|---|---|---|---|---|---|
| Number of Reports | 18,141 | 16,398 | 20,147 | 46,942 | 50,801 |

The total number of reports received in FY2021 was 50,801, increasing 8% compared to 46,942 in the previous year. [Figure 3] shows the change in the total number of reports in the past 5 years.



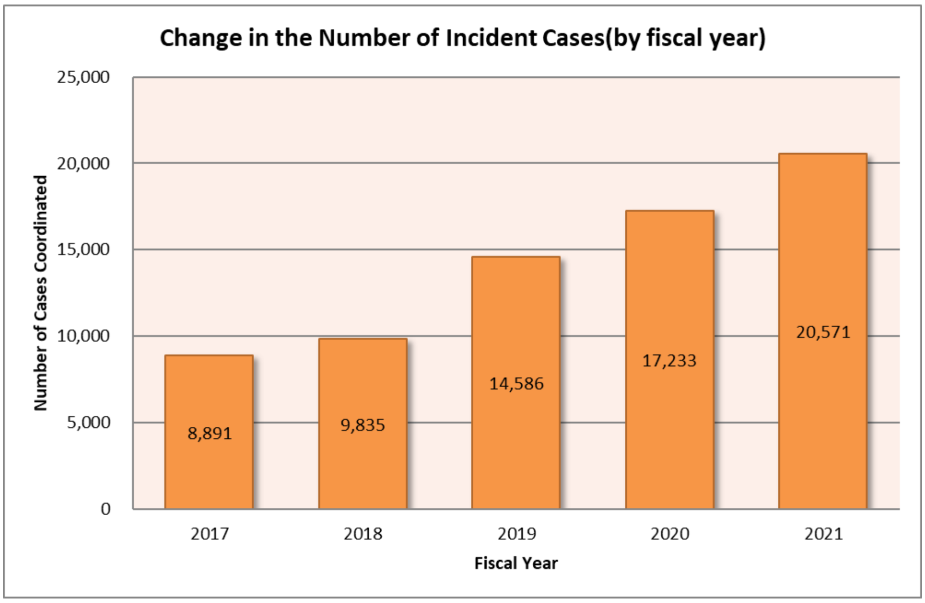
[Figure 3 : Change in the total number of reports (by fiscal year)]

[Chart 3] shows the number of cases coordinated in each fiscal year over the past 5 years including FY2021.

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

| FY | 2017 | 2018 | 2019 | 2020 | 2021 |
|---|---|---|---|---|---|
| Number of Cases Coordinated | 8,891 | 9,835 | 14,586 | 17,233 | 20,571 |

The total number of cases coordinated in FY2021 was 20,571, increasing 19% year on year from 17,233. [Figure 4] shows the change in the total number of cases coordinated in the past 5 years.

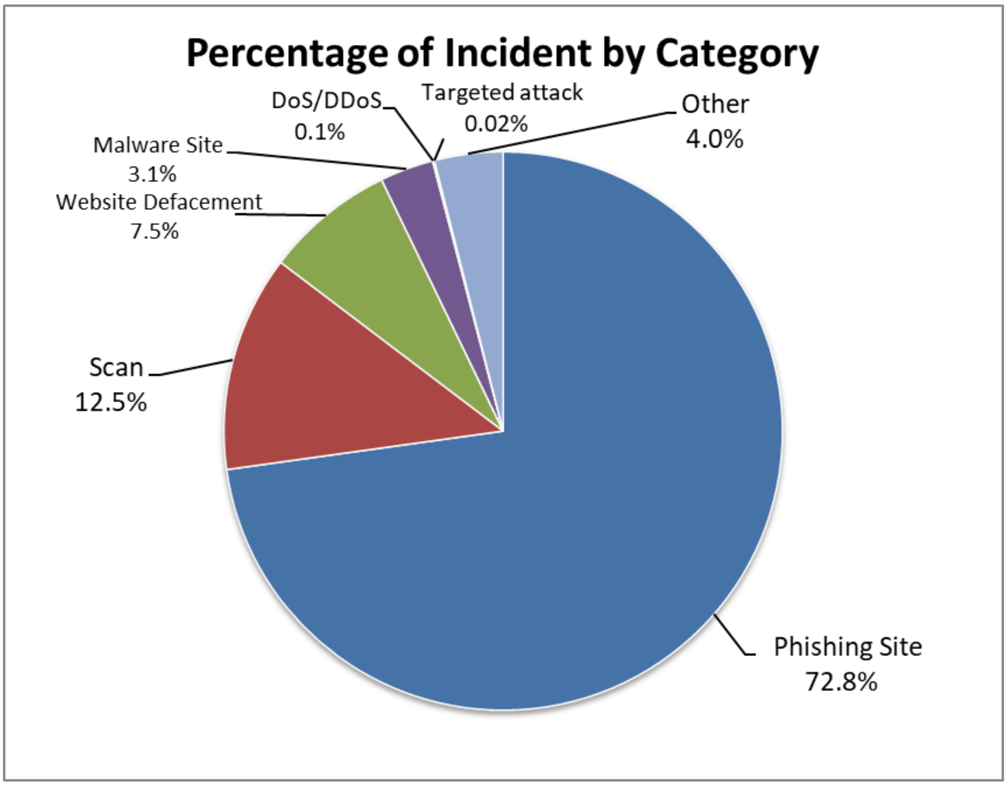


[Figure 4: Change in the total number of cases coordinated (by fiscal year)]

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]

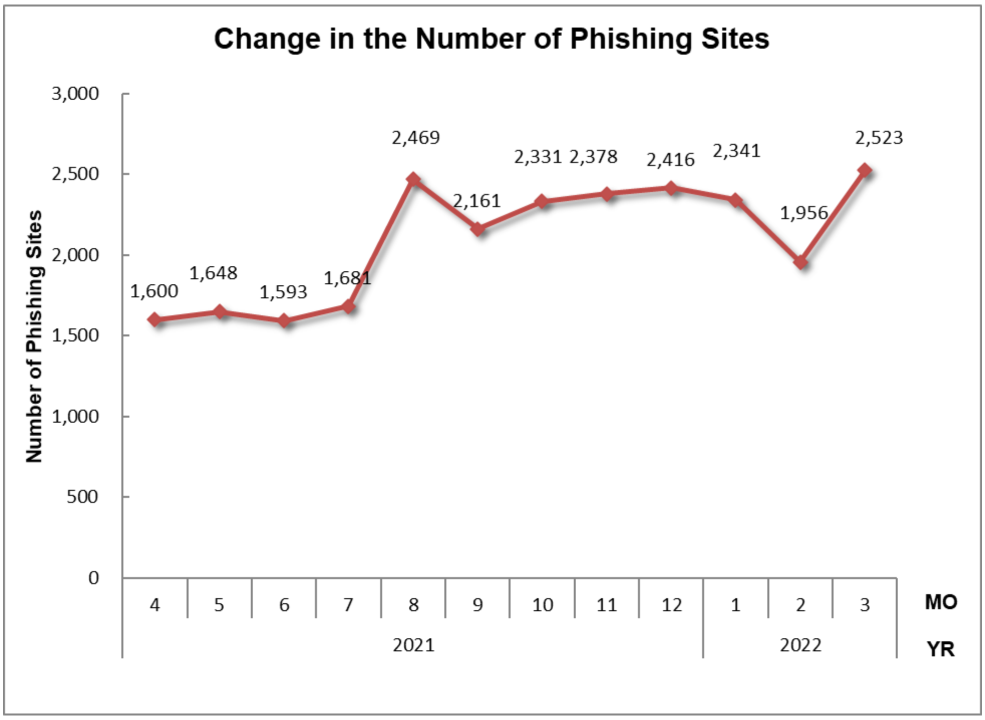
| Incident Category | Jan | Feb | Mar | Total | Last Qtr. Total |
|---|---|---|---|---|---|
| Phishing Site | 2,341 | 1,956 | 2,523 | 6,820 | 7,125 |
| Website Defacement | 164 | 250 | 289 | 703 | 906 |
| Malware Site | 104 | 80 | 107 | 291 | 406 |
| Scan | 370 | 474 | 330 | 1,174 | 1,011 |
| DoS/DDoS | 0 | 1 | 6 | 7 | 16 |
| ICS Related | 0 | 0 | 0 | 0 | 0 |
| Targeted attack | 0 | 0 | 2 | 2 | 1 |
| Other | 104 | 129 | 139 | 372 | 342 |



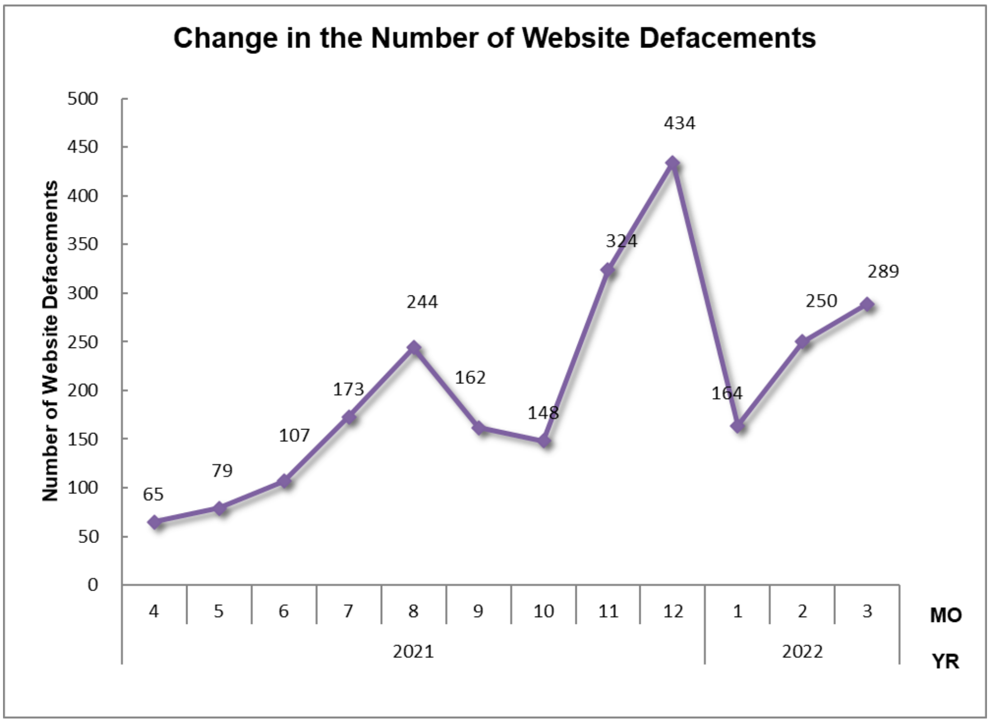
[Figure 5 : Percentage of incidents by category]

Incidents categorized as phishing sites accounted for 72.8%, and those categorized as scans, which search for vulnerabilities in systems, made up 12.5%.

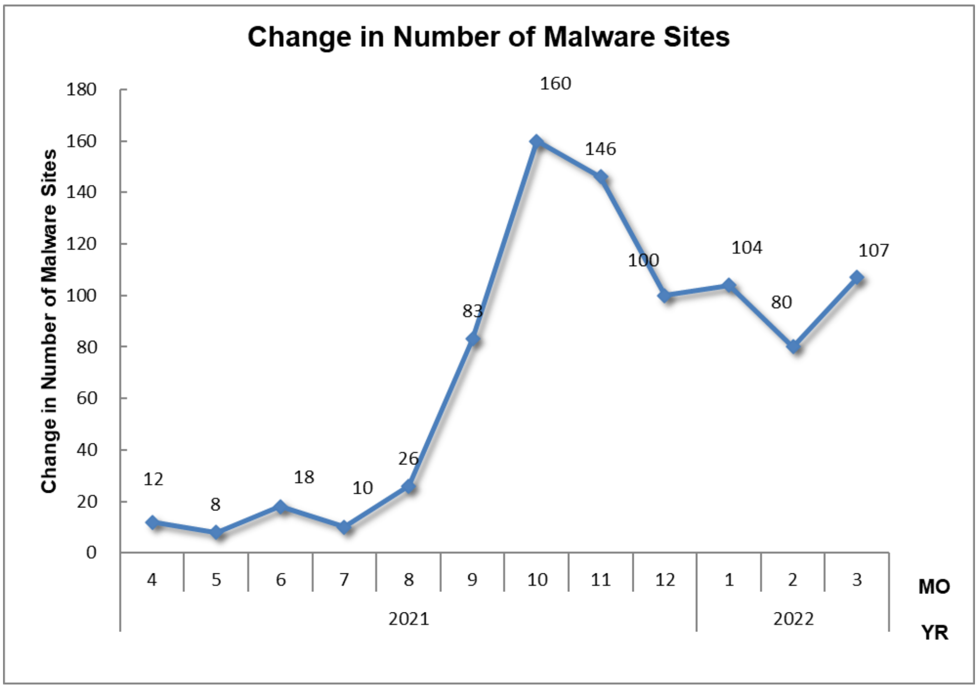
[Figure 6] through [Figure 9] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



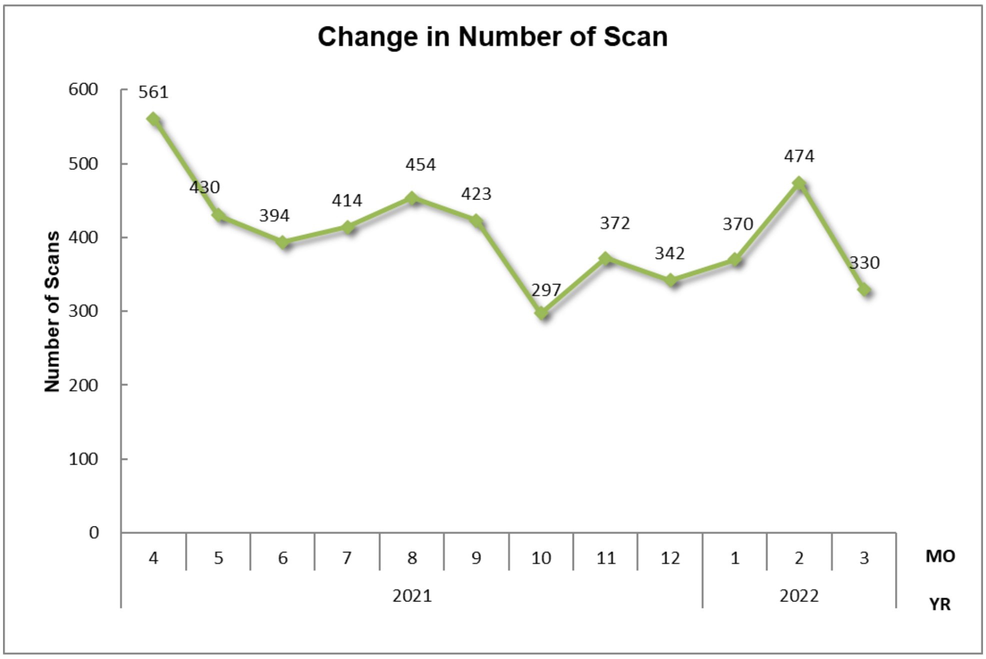
[Figure 6：Change in the number of phishing sites]



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

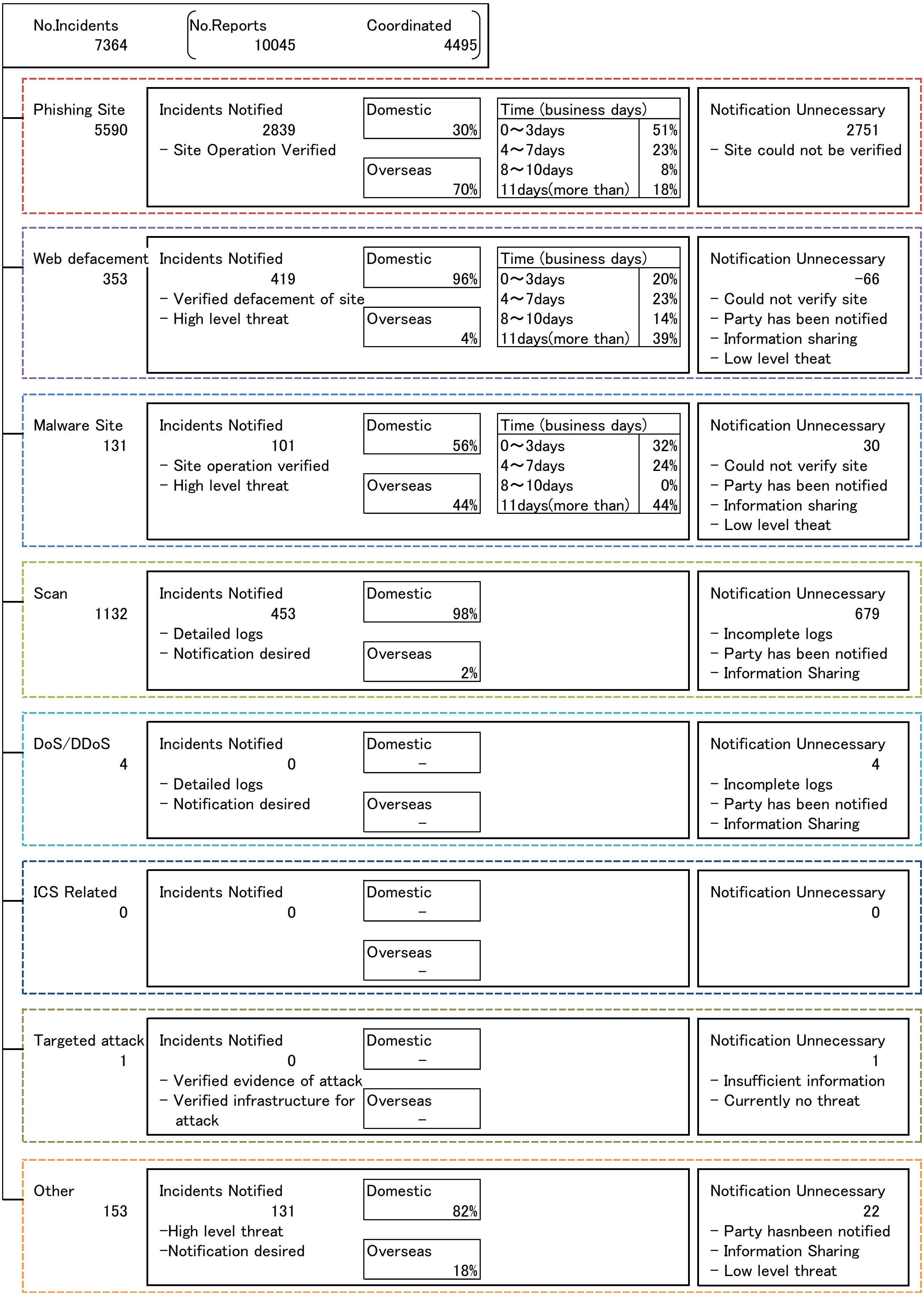


[Figure 8：Change in the number of malware sites]



[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



No.Incidents 7364

No.Reports 10045 Coordinated 4495

| | | | | |
|---|---|---|---|---|
| Phishing Site<br>5590 | Incidents Notified<br>2839<br>－ Site Operation Verified | Domestic<br>30%<br>Overseas<br>70% | Time (business days)<br>0～3days 51%<br>4～7days 23%<br>8～10days 8%<br>11days(more than) 18% | Notification Unnecessary<br>2751<br>－ Site could not be verified |
| Web defacement<br>353 | Incidents Notified<br>419<br>－ Verified defacement of site<br>－ High level threat | Domestic<br>96%<br>Overseas<br>4% | Time (business days)<br>0～3days 20%<br>4～7days 23%<br>8～10days 14%<br>11days(more than) 39% | Notification Unnecessary<br>－66<br>－ Could not verify site<br>－ Party has been notified<br>－ Information sharing<br>－ Low level theat |
| Malware Site<br>131 | Incidents Notified<br>101<br>－ Site operation verified<br>－ High level threat | Domestic<br>56%<br>Overseas<br>44% | Time (business days)<br>0～3days 32%<br>4～7days 24%<br>8～10days 0%<br>11days(more than) 44% | Notification Unnecessary<br>30<br>－ Could not verify site<br>－ Party has been notified<br>－ Information sharing<br>－ Low level theat |
| Scan<br>1132 | Incidents Notified<br>453<br>－ Detailed logs<br>－ Notification desired | Domestic<br>98%<br>Overseas<br>2% | | Notification Unnecessary<br>679<br>－ Incomplete logs<br>－ Party has been notified<br>－ Information Sharing |
| DoS/DDoS<br>4 | Incidents Notified<br>0<br>－ Detailed logs<br>－ Notification desired | Domestic<br>－<br>Overseas<br>－ | | Notification Unnecessary<br>4<br>－ Incomplete logs<br>－ Party has been notified<br>－ Information Sharing |
| ICS Related<br>0 | Incidents Notified<br>0 | Domestic<br>－<br>Overseas<br>－ | | Notification Unnecessary<br>0 |
| Targeted attack<br>1 | Incidents Notified<br>0<br>－ Verified evidence of attack<br>－ Verified infrastructure for attack | Domestic<br>－<br>Overseas<br>－ | | Notification Unnecessary<br>1<br>－ Insufficient information<br>－ Currently no threat |
| Other<br>153 | Incidents Notified<br>131<br>－High level threat<br>－Notification desired | Domestic<br>82%<br>Overseas<br>18% | | Notification Unnecessary<br>22<br>－ Party hasnbeen notified<br>－ Information Sharing<br>－ Low level threat |

[Figure 10：Breakdown of incidents coordinated/handled]

## 3. Incident Trends

### 3.1. Phishing Site Trends

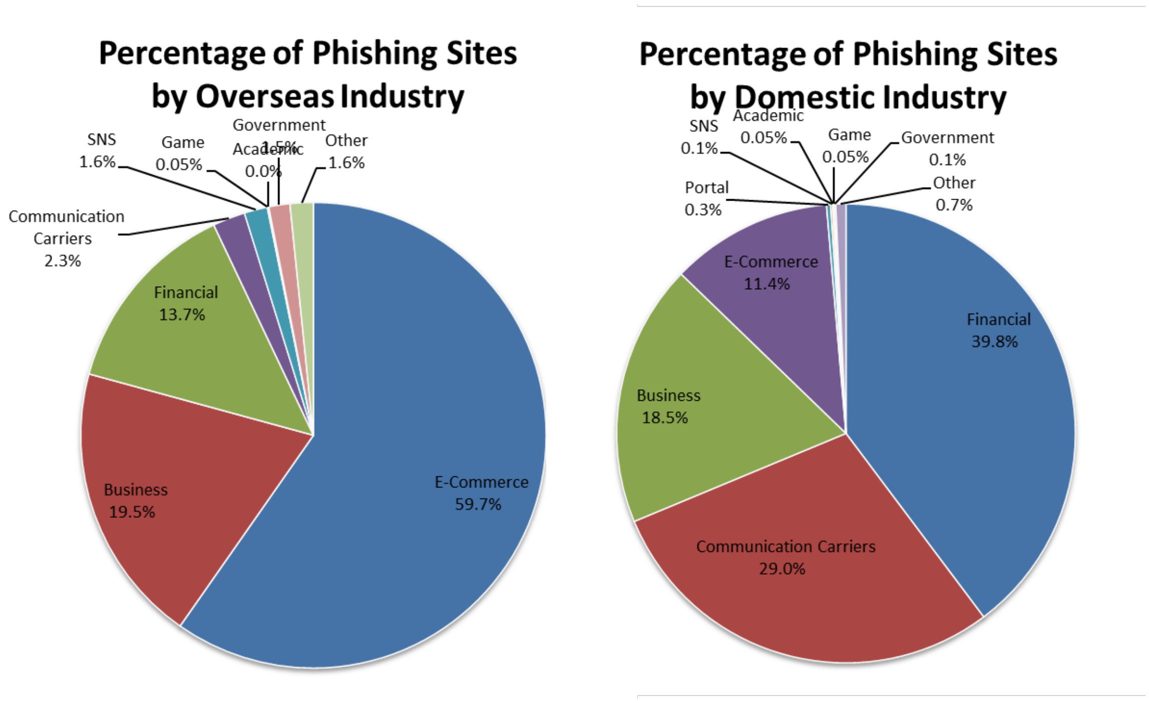
During this quarter, 6,820 reports on phishing sites were received, representing a 4% decrease from 7,125 in the previous quarter. This marks a 41% increase from the same quarter last year (4,831).

During this quarter, there were 4,196 phishing sites that spoofed domestic brands, increasing 6% from 3,962 in the previous quarter. There were 2,043 phishing sites that spoofed overseas brands, decreasing 15% from 2,406 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 | 1,427 | 1,022 | 1,747 | 4,196（62%） |
| Overseas Brand | 721 | 771 | 551 | 2,043（30%） |
| Unknown Brand [*5] | 193 | 163 | 225 | 581 （9%） |
| Monthly Total | 2,341 | 1,956 | 2,523 | 6,820 |

[*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, 59.7% spoofed e-commerce websites for overseas brands and 39.8% spoofed financial institution websites for domestic brands, both representing the largest share respectively.

Among the phishing sites reported for domestic brands, those targeting mobile carrier users accounted for a significant proportion. Phishing sites spoofing Electronic Toll System (ETC) usage inquiry services and the member login pages of e-commerce websites continued to be seen in large numbers as in the previous quarter.
In March, reports of phishing sites spoofing Eki-Net, a website provided by East Japan Railway Company, increased.

As for overseas brands, phishing sites spoofing the login page of online shopping sites accounted for more than half the total, and the brands and the number of reports have remained largely unchanged from the previous quarter.

The websites that JPCERT/CC coordinated with to suspend phishing sites were 62% domestic and 30% overseas for this quarter, indicating an increase in domestic parties compared to the previous quarter (domestic: 23%, overseas: 77%).

### 3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 703. This was a 22% decrease from 906 in the previous quarter.

During this quarter, JPCERT/CC continued to receive multiple reports of redirection from compromised websites to suspicious websites. Cases in which multiple websites were compromised simultaneously were observed on hosts where multiple websites were administered using VirtualHost. This could have been carried out by first altering one website and then spreading the compromise to other websites using the following steps.

Attack steps

1. Use vulnerabilities in CMS, etc. to alter the first website and plant a WebShell
2. Use the WebShell to place a tool for increasing permission levels on the website, and then launch the tool to gain root permission
3. Use the root permission to compromise multiple websites on the same host

When there are multiple websites on the same host, a vulnerability in the content of one website could be exploited to compromise other websites on the same host.

### 3.3. Targeted Attack Trends

There were 2 incidents categorized as a targeted attack.
The incident identified is described below.

(1) Attacks using a shortcut file that initiates a download of JavaScript

This quarter, JPCERT/CC received a report of an attack targeting an employee of a financial institution. The method identified used the hijacked LinkedIn account of a cryptocurrency exchange employee to send a malicious ZIP file to the target financial institution employee with the aim of infecting the target's computer with malware. The ZIP file contained a shortcut file that downloads and executes malicious JavaScript. This attack resembles the attack campaign discussed in the following article published on JPCERT/CC's official blog, indicating that attack activities are still being carried out.

JPCERT/CC Eyes: Spear Phishing against Cryptocurrency Businesses
https://blogs.jpcert.or.jp/en/2019/07/spear-phishing-against-cryptocurrency-businesses.html

### 3.4. Other Incident Trends

The number of malware sites reported in this quarter was 291. This was a 28% decrease from 406 in the previous quarter.

The number of scans reported in this quarter was 1,174. This was a 16% increase from 1,011 in the previous quarter. A breakdown of the ports that were scanned are listed in [Chart 6]. Ports targeted frequently were SSH (22/TCP), Telnet (23/TCP) and 143/TCP.

[Chart 6：Number of scans by port]

| Port | Jan | Feb | Mar | Total |
|---|---|---|---|---|
| 22/tcp | 102 | 136 | 119 | 357 |
| 23/tcp | 51 | 186 | 81 | 318 |
| 143/tcp | 112 | 71 | 51 | 234 |
| 80/tcp | 53 | 29 | 35 | 117 |
| 37215/tcp | 13 | 48 | 30 | 91 |
| 25/tcp | 12 | 9 | 15 | 36 |
| 52869/tcp | 4 | 15 | 2 | 21 |
| 2323/tcp | 9 | 4 | 5 | 18 |
| 443/tcp | 3 | 5 | 0 | 8 |
| 21/tcp | 3 | 3 | 1 | 7 |
| 6379/tcp | 3 | 1 | 2 | 6 |
| 3389/tcp | 3 | 0 | 1 | 4 |
| 3306/tcp | 3 | 0 | 1 | 4 |
| 5555/tcp | 1 | 2 | 0 | 3 |
| 445/tcp | 0 | 3 | 0 | 3 |
| 8081/tcp | 2 | 0 | 0 | 2 |
| 1433/tcp | 1 | 1 | 0 | 2 |
| 110/tcp | 2 | 0 | 0 | 2 |
| 9443/tcp | 1 | 0 | 0 | 1 |
| Unknown | 9 | 5 | 3 | 17 |
| Monthly Total | 387 | 518 | 346 | 1251 |

There were 372 incidents categorized as other. This was a 9% increase from 342 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 human-operated ransomware attacks

This quarter, JPCERT/CC received a number of reports of human-operated ransomware attacks. JPCERT/CC has interviewed the victims to obtain information on the scope of damage, status of investigation and status of response at the time of report, then based on that information, identified the type of related ransomware attacks and provided such information as intrusion methods so that it can be used to take countermeasures and advice on how to respond. In many of the cases identified, vulnerabilities in SSL-VPN products and Log4j were apparently exploited to breach the network. Some of the groups reported as carrying out human-operated ransomware attacks include FiveHands, Pandra and Robinhood.

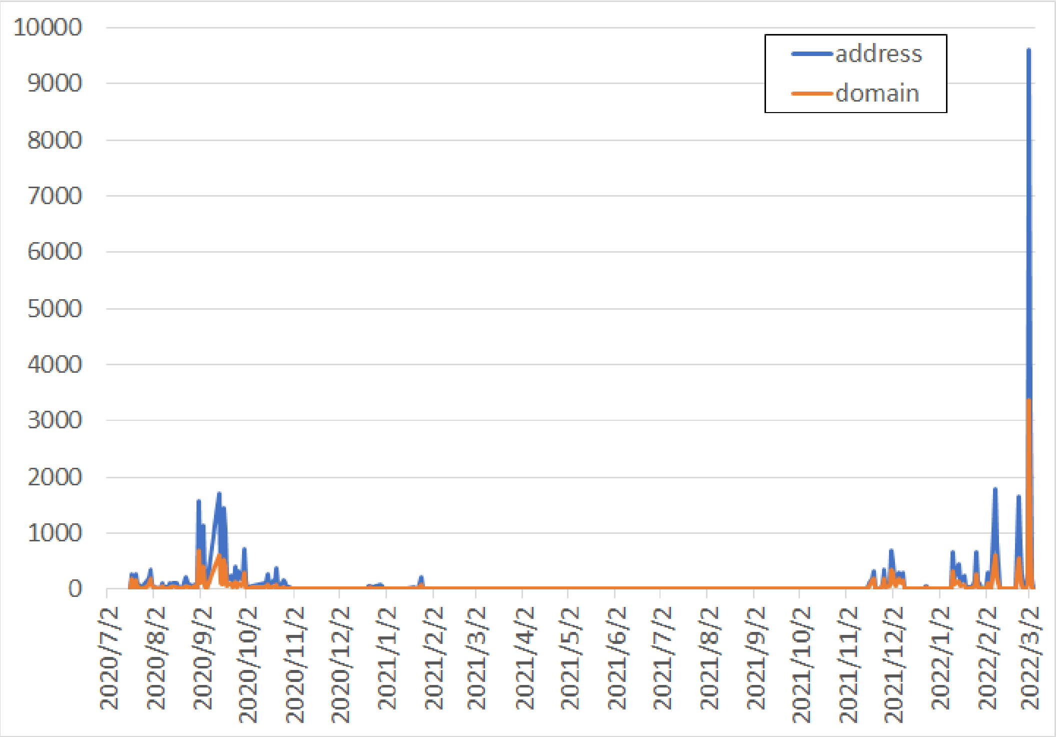
JPCERT/CC organized the insights gained through these activities with a focus on initial incident response and made them available as "FAQ to Read When Subjected to A Human-Operated Ransomware Attack" (Japanese). JPCERT/CC also released a video that summarizes the key points of initial response to a human-operated ransomware attack.

FAQ to Read When Subjected to A Human-Operated Ransomware Attack (Japanese)
https://www.jpcert.or.jp/magazine/security/ransom-faq.html

Key Points of Initial Response to a Human-Operated Ransomware Attack (YouTube) (Japanese)
https://www.youtube.com/watch?v=nDOSn_ss7zI

(2) Coordination involving reports of Emotet malware

This quarter, JPCERT/CC continued to receive numerous reports related to Emotet. The number of reports has increased particularly since February, along with the number of infected computers in Japan. Changes in the numbers of computers infected with Emotet in Japan based on information provided to JPCERT/CC are shown in [Figure 12].



[Figure 12：Changes in the numbers of computers and organizations infected with Emotet in Japan]

Given the recent spread of infections in Japan, JPCERT/CC issued the following security alert and released a video providing an overview of the Emotet malware and explaining how to check for infection.

Alert Regarding Re-emergence of Emotet Malware Infection Activities
https://www.jpcert.or.jp/english/at/2022/at220006.html

Emotet Malware Infections Spreading in Japan (YouTube) (Japanese)
https://www.youtube.com/watch?v=wvu9sWiB2_U

How to check Emotet infection and respond (YouTube) (Japanese)
https://www.youtube.com/watch?v=nqxikr1x2ag

## 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 2021.

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