JPCERT/CC Incident Handling Report

October 1, 2021 ～ December 31, 2021

JPCERT Coordination Center
January 20, 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 October 1, 2021 through December 31, 2021.

[*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]	2,834	4,170	4,866	11,870	12,469
Number of Incident [*3]	3,045	3,302	3,460	9,807	8,786
Cases Coordinated [*4]	1,995	2,163	2,396	6,554	4,714

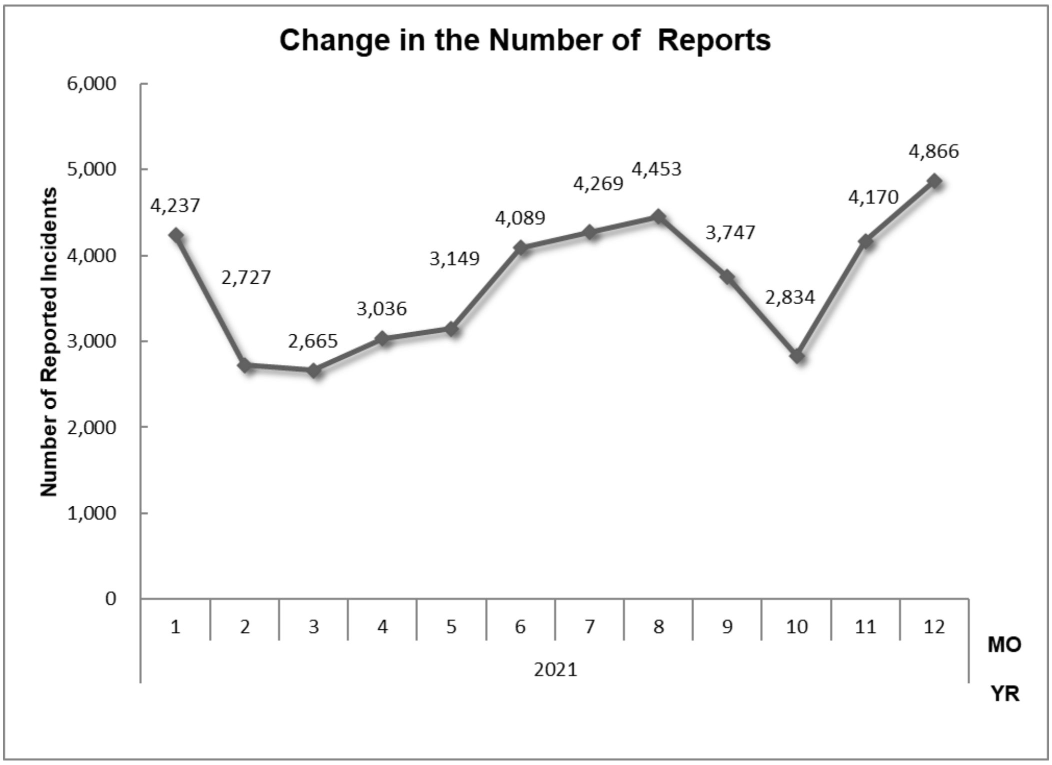
[*2] "Number of Reports" refers to the total number of reports sent through the web form, e-mail or FAX.

[*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.

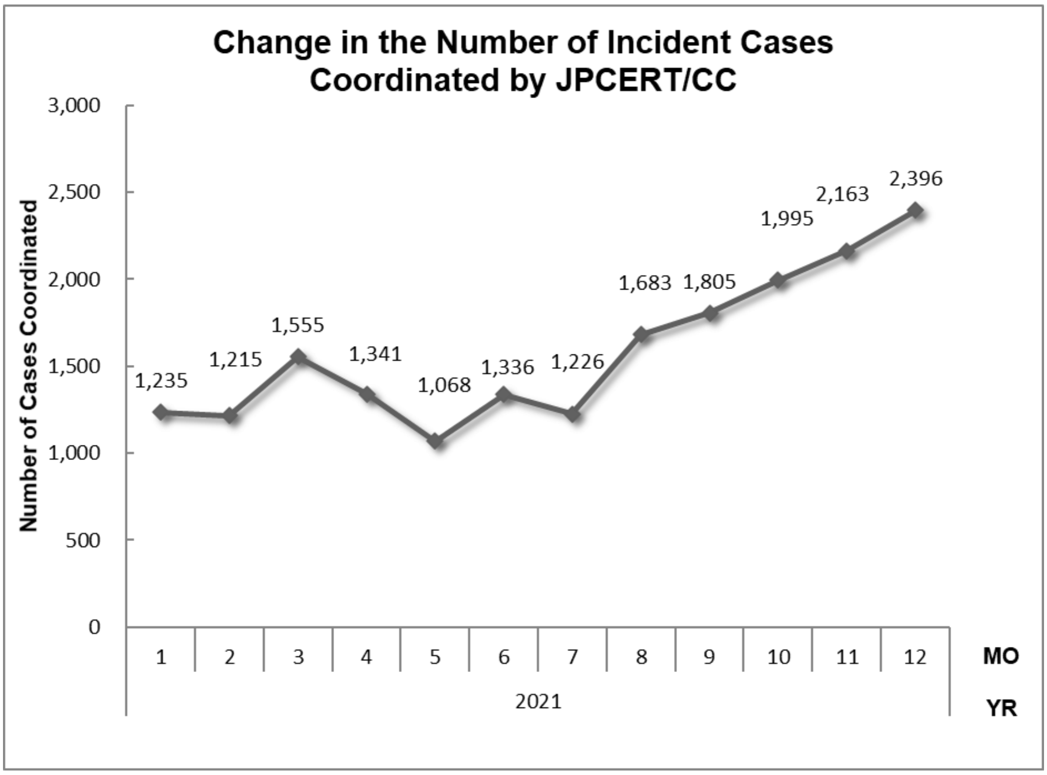
[*4] "Number of Cases Coordinated" refers to the number of cases where coordination took place to prevent the spreading of an incident by sending them a report and asking the site administrator to address any issues.

The total number of reports received in this quarter was 11,870. Of these, the number of domestic and overseas organizations that JPCERT/CC coordinated with was 6,554. When compared with the previous quarter, the total number of reports decreased by 5%, and the number of cases coordinated increased by 39%. Year on year, the number of reports decreased by 9%, and the number of cases coordinated increased by 55%.

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



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

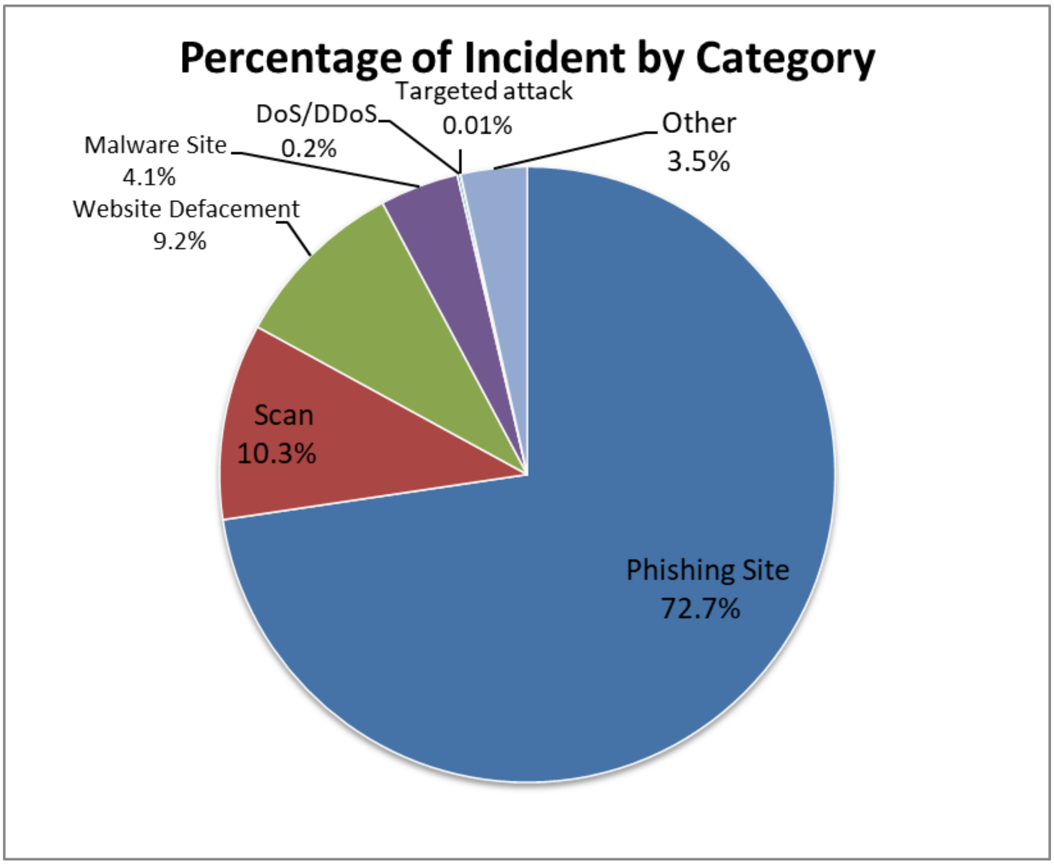


[Figure 2: Change in the number of incident cases coordinated]

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 the number of incidents received per category in this quarter. The breakdown in percentage is shown in [Figure 3].

[Chart 2: Number of incidents by category]

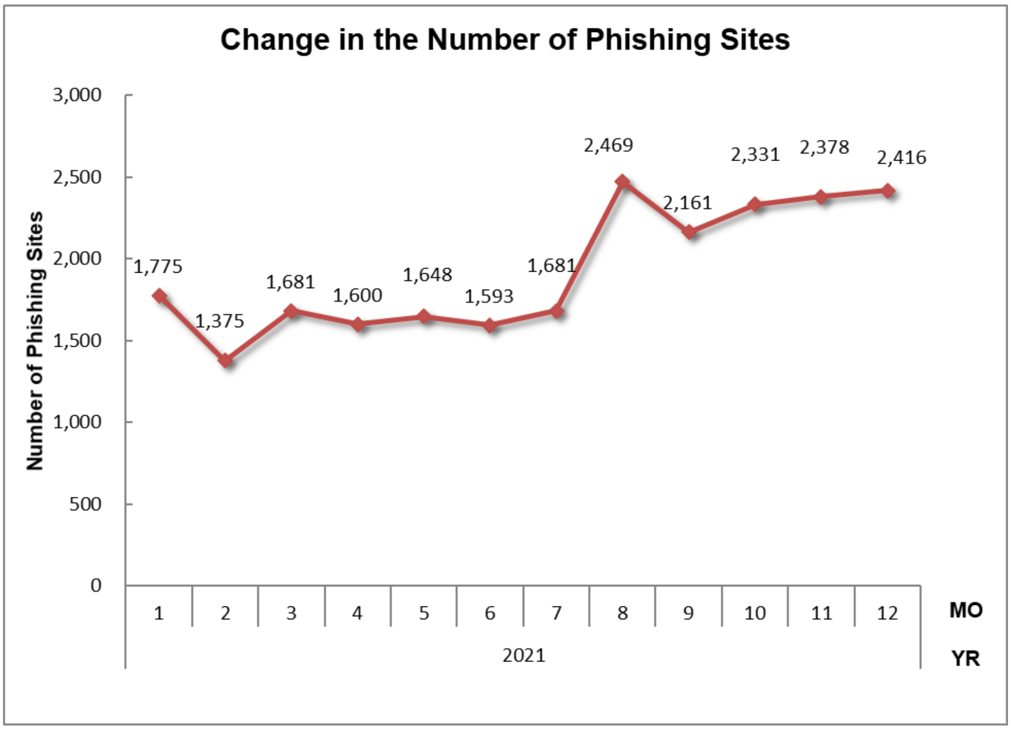
Incident Category	Oct	Nov	Dec	Total	Last Qtr. Total
Phishing Site	2,331	2,378	2,416	7,125	6,311
Website Defacement	148	324	434	906	579
Malware Site	160	146	100	406	119
Scan	297	372	342	1,011	1,291
DoS/DDoS	12	2	2	16	7
ICS Related	0	0	0	0	0
Targeted attack	1	0	0	1	4
Other	96	80	166	342	475



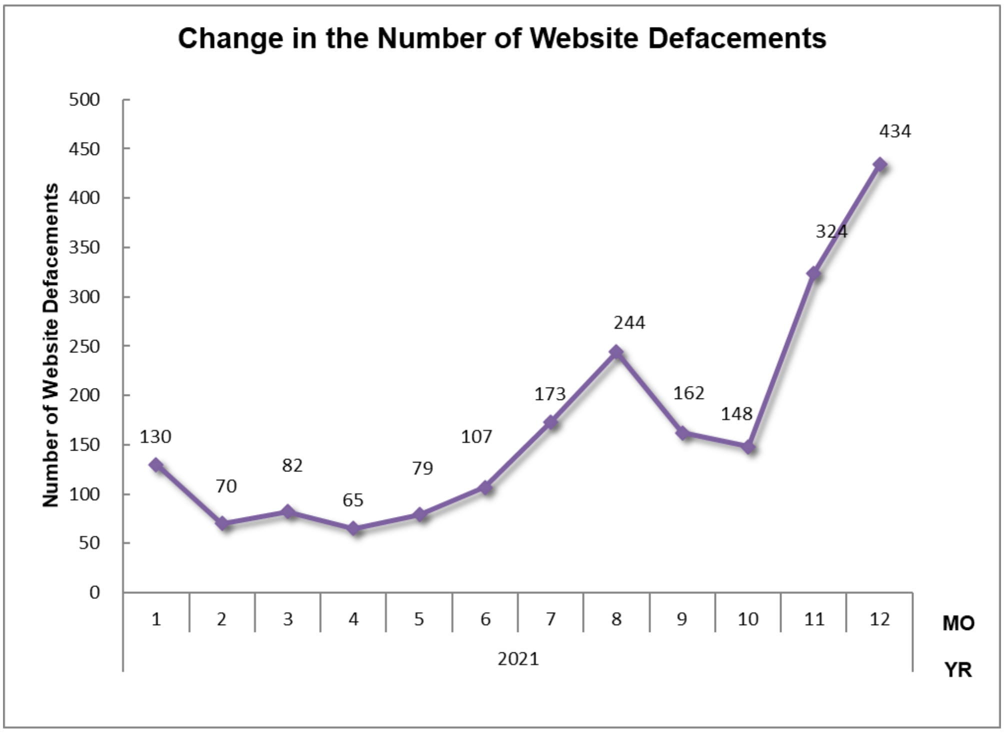
[Figure 3: Percentage of incidents by category]

Incidents categorized as phishing sites accounted for 72.7%, and those categorized as scans, which search for vulnerabilities in systems, made up 10.3%.

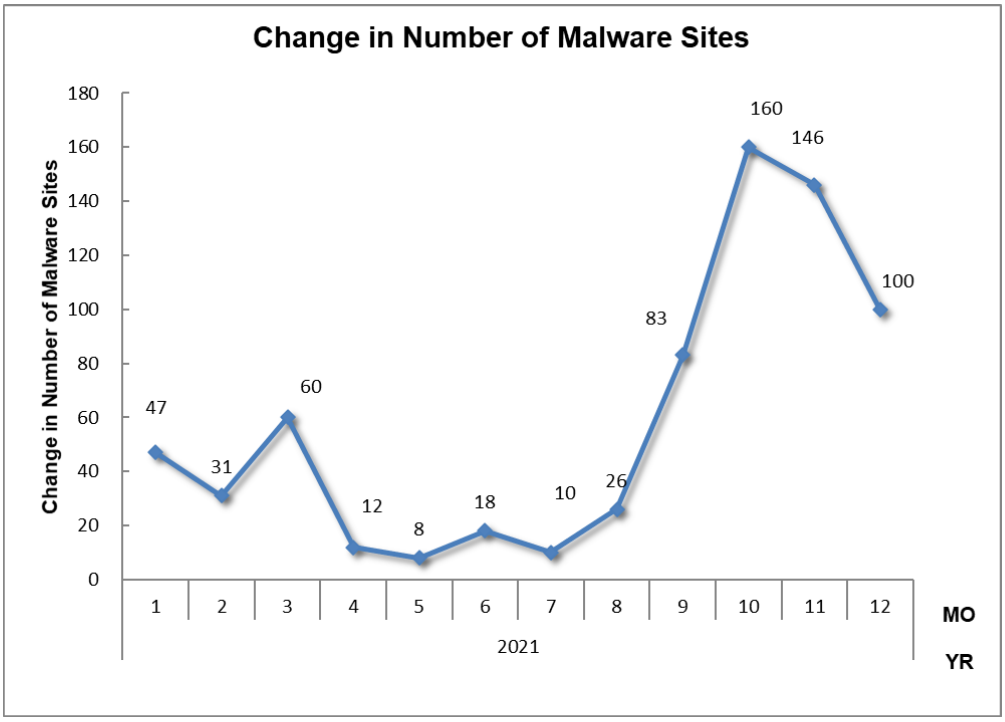
[Figure 4] through [Figure 7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



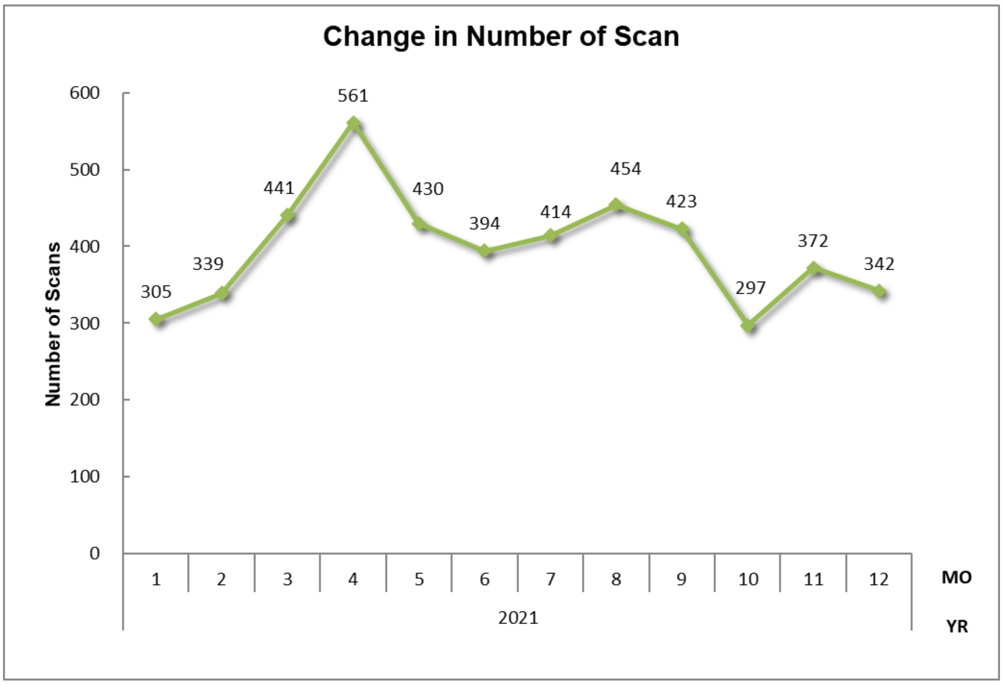
[Figure 4: Change in the number of phishing sites]



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

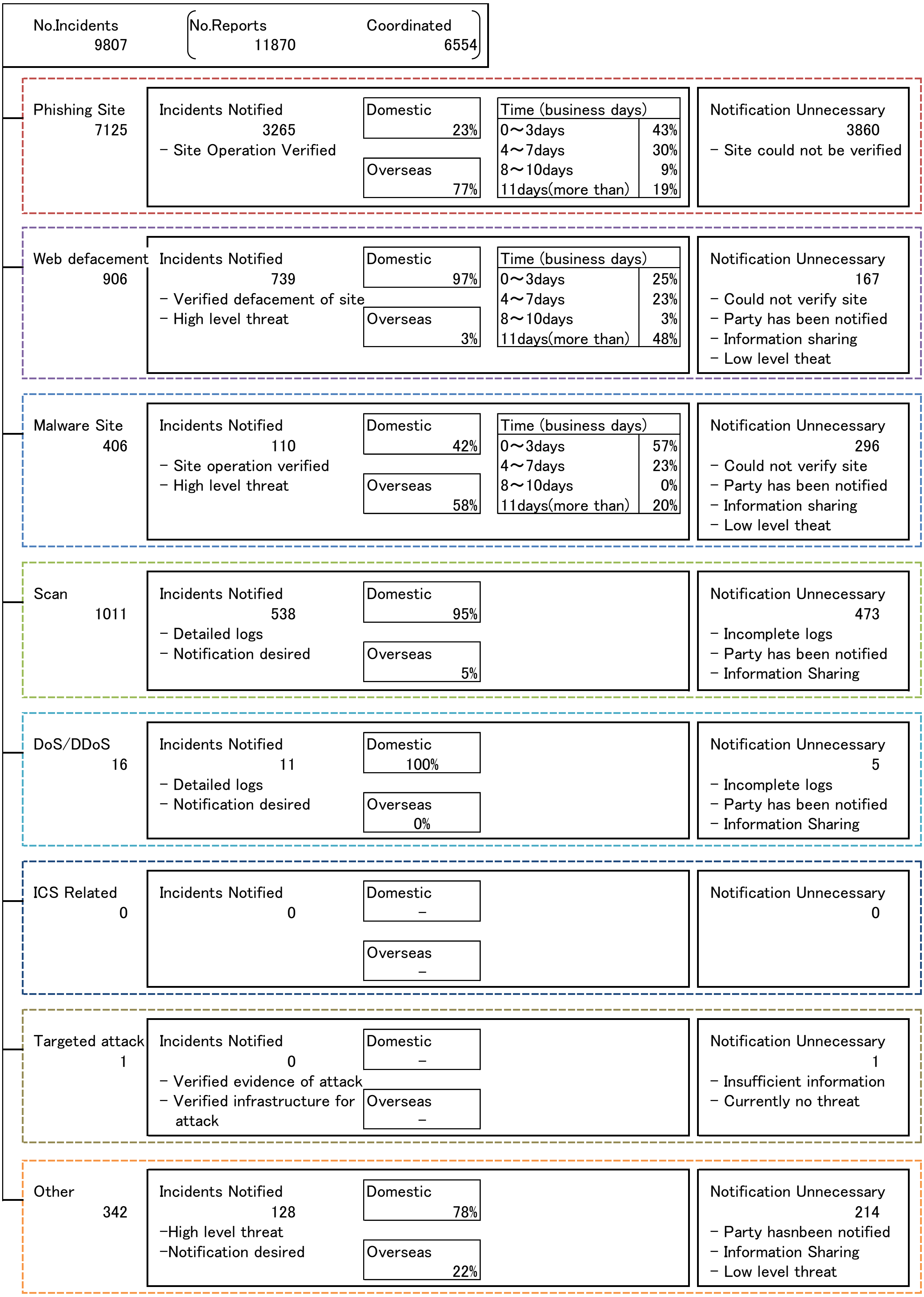


[Figure 6: Change in the number of malware sites]



[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.



No.Incidents 9807

No.Reports 11870

Coordinated 6554

Phishing Site 7125

Incidents Notified 3265
- Site Operation Verified

Domestic 23%

Overseas 77%

Time (business days)	
0～3days	43%
4～7days	30%
8～10days	9%
11days(more than)	19%

Notification Unnecessary 3860
- Site could not be verified

Web defacement 906

Incidents Notified 739
- Verified defacement of site
- High level threat

Domestic 97%

Overseas 3%

Time (business days)	
0～3days	25%
4～7days	23%
8～10days	3%
11days(more than)	48%

Notification Unnecessary 167
- Could not verify site
- Party has been notified
- Information sharing
- Low level theat

Malware Site 406

Incidents Notified 110
- Site operation verified
- High level threat

Domestic 42%

Overseas 58%

Time (business days)	
0～3days	57%
4～7days	23%
8～10days	0%
11days(more than)	20%

Notification Unnecessary 296
- Could not verify site
- Party has been notified
- Information sharing
- Low level theat

Scan 1011

Incidents Notified 538
- Detailed logs
- Notification desired

Domestic 95%

Overseas 5%

Notification Unnecessary 473
- Incomplete logs
- Party has been notified
- Information Sharing

DoS/DDoS 16

Incidents Notified 11
- Detailed logs
- Notification desired

Domestic 100%

Overseas 0%

Notification Unnecessary 5
- Incomplete logs
- Party has been notified
- Information Sharing

ICS Related 0

Incidents Notified 0

Domestic –

Overseas –

Notification Unnecessary 0

Targeted attack 1

Incidents Notified 0
- Verified evidence of attack
- Verified infrastructure for attack

Domestic –

Overseas –

Notification Unnecessary 1
- Insufficient information
- Currently no threat

Other 342

Incidents Notified 128
-High level threat
-Notification desired

Domestic 78%

Overseas 22%

Notification Unnecessary 214
- Party hasnbeen notified
- Information Sharing
- Low level threat

[Figure 8: Breakdown of incidents coordinated/handled]

3. Incident Trends

3.1. Phishing Site Trends

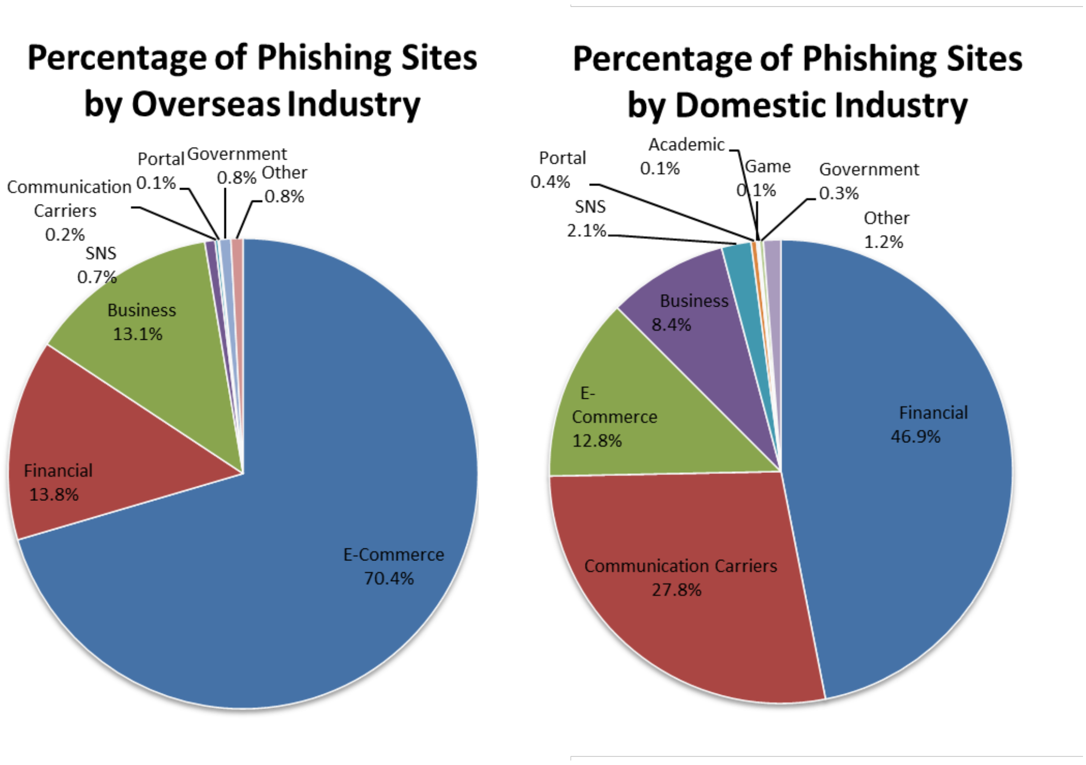
During this quarter, 7,125 reports on phishing sites were received, representing a 13% increase from 6,311 in the previous quarter. This marks a 42% increase from the same quarter last year (5,015).

During this quarter, there were 3,962 phishing sites that spoofed domestic brands, increasing 12% from 3,533 in the previous quarter. There were 2,406 phishing sites that spoofed overseas brands, increasing 53% from 1,570 in the previous quarter. The breakdown of the brand type (domestic, overseas) that the phishing sites spoofed in this quarter is shown in [Chart 3], and a breakdown by industry for domestic and overseas brands is 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	1,395	1,203	1,364	3,962（56%）
Overseas Brand	732	839	835	2,406（34%）
Unknown Brand [*5]	204	336	217	757（11%）
Monthly Total	2,331	2,378	2,416	7,125

[*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, 70.4% spoofed e-commerce websites for overseas brands and 46.9% spoofed financial institution websites for domestic brands, both representing the largest share respectively.

Among the phishing sites reported for domestic brands, those spoofing Electronic Toll System (ETC) usage inquiry services and the member login pages of e-commerce websites have increased. Phishing sites of ETC usage inquiry services grew by 6 times while those spoofing e-commerce websites increased tenfold, both growing significantly from the previous quarter.

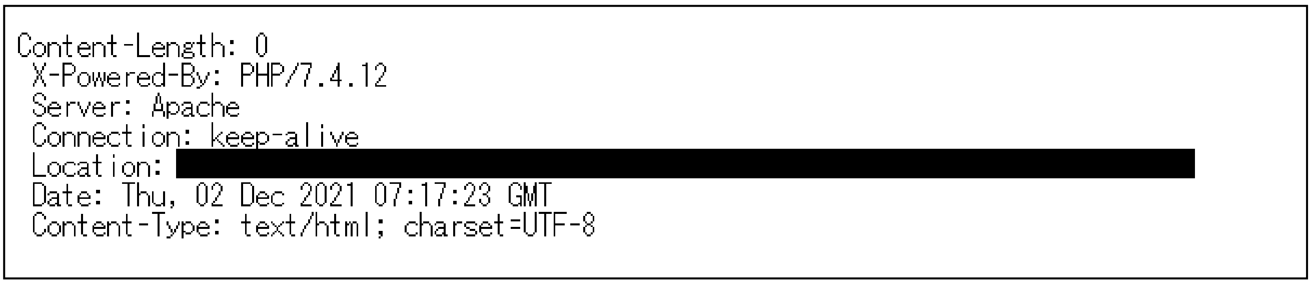
As for overseas brands, phishing sites spoofing the login page of online shopping sites accounted for more than half the total, and the top brands in terms of the number of reports have remained unchanged.

The websites that JPCERT/CC coordinated with to take down phishing sites were 23% domestic and 77% overseas for this quarter, indicating the same proportion as the previous quarter (domestic: 23%, overseas: 77%).

3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 906. This was a 56% increase from 579 in the previous quarter.

During this quarter, JPCERT/CC continued to receive multiple reports of redirection from compromised websites to suspicious websites. When visitors access a compromised website, they receive a response with a Location header inserted as shown in [Figure 10] which redirects them to a suspicious website. This redirection takes place only when the UserAgent at the time of access is the Safari browser on iOS.



```
Content-Length: 0
 X-Powered-By: PHP/7.4.12
 Server: Apache
 Connection: keep-alive
 Location: [redacted]
 Date: Thu, 02 Dec 2021 07:17:23 GMT
 Content-Type: text/html; charset=UTF-8
```

[Figure 10: Example of a malicious Location header]

In addition, JPCERT/CC continued to receive reports of websites redirecting visitors to a lucky visitor scam page due to a malicious PHP script planted in a compromised website, which was also reported in the previous quarter. Details of this attack are discussed on JPCERT/CC Eyes. For more information, please access the following web page.

PHP Malware Used in Lucky Visitor Scam
https://blogs.jpcert.or.jp/en/2021/06/php_malware.html

3.3. Targeted Attack Trends

There was 1 incident categorized as a targeted attack. The incident identified is described below.

(1) Attacks related to a malware campaign called “AppleJeus”
This quarter, JPCERT/CC received reports of targeted attacks related to a malware campaign called AppleJeus. In these attacks, the attacker contacts employees of a target organization via LinkedIn, directing them to run an installer embedded with malware. Running this installer causes infection with malware called UnionCrypto[1].

3.4. Other Incident Trends

The number of malware sites reported in this quarter was 406. This was a 241% increase from 119 in the previous quarter.

The number of scans reported in this quarter was 1,011. This was a 21.7% decrease from 1,291 in the previous quarter. A breakdown of the ports that were scanned are listed in [Chart 4].Ports targeted frequently were Telnet (23/TCP), SSH (22/TCP) and 37215/TCP.

[Chart 4: Number of scans by port]

Port	Oct	Nov	Dec	Total
23/tcp	115	131	102	348
22/tcp	85	93	54	232
37215/tcp	18	70	32	120
143/tcp	27	29	53	109
80/tcp	23	25	55	103
2323/tcp	22	17	11	50
25/tcp	6	4	21	31
52869/tcp	4	15	1	20
26/tcp	0	7	1	8
6379/tcp	2	4	0	6
443/tcp	1	0	5	6
3389/tcp	1	3	2	6
3306/tcp	3	0	3	6
445/tcp	0	1	3	4
21/tcp	2	2	0	4
81/tcp	0	1	2	3
8081/tcp	1	1	1	3
Unknown	16	10	19	45
Monthly Total	326	413	365	1,104

There were 342 incidents categorized as other. This was a 28% decrease from 475 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 on website defacements exploiting a vulnerability (CVE-2021-20837) in Movable Type

JPCERT/CC received multiple reports on website defacements exploiting a vulnerability (CVE-2021-20837) in Movable Type published on October 20, 2021. JPCERT/CC analyzed access logs of web servers and files that may have been planted by a third party, and confirmed that PHP backdoors (FoxWSO, etc.) commonly seen in compromised websites were created.
Some of the affected websites were subject to the recent attacks since they had left the Movable Type system used in the past on the website, even though they were created using other content management systems.

These attacks can be countered by updating Movable Type to the latest version. Users of Movable Type should read the following alert and take appropriate steps.

Alert Regarding Vulnerability (CVE-2021-20837) in Movable Type XMLRPC API
https://www.jpcert.or.jp/english/at/2021/at210047.html

(2) Coordination involving reports of ransomware infections

This quarter, JPCERT/CC received multiple reports of ransomware infections involving Snatch, AvosLocker, Magniber, Ragnar Locker and so on. 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, provided such information as the characteristics of the relevant ransomware attack and advice on how to respond.

(3) Coordination involving hosts that may be affected by a vulnerability (CVE-2021-44228) in Apache Log4j

JPCERT/CC received information from an external organization on domestic hosts still affected by the following Apache Log4j vulnerability published on December 11, 2021.

Alert Regarding Arbitrary Code Execution Vulnerability (CVE-2021-44228) in Apache Log4j
https://www.jpcert.or.jp/english/at/2021/at210050.html

There were about 150 hosts affected, and while many of them had the vulnerability contained in a product, some were affected due to a vulnerable cloud service. Based on this information, JPCERT/CC contacted operators managing the relevant IP addresses in Japan, and asked them to see if their hosts were affected and take necessary measures if they were using a vulnerable system.

5. References

(1)The Cybersecurity and Infrastructure Security Agency
MAR-10322463-3.v1 - AppleJeus: Union Crypto
https://www.cisa.gov/uscert/ncas/analysis-reports/ar21-048c

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 Fiscal Year".

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