JPCERT CC®

JPCERT/CC Incident Handling Report

October 1, 2020 ～ December 31, 2020

JPCERT Coordination Center
January 21, 2021

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, 2020 December 31, 2020.

[*1] JPCERT/CC refers to all events that may occur in the management of information systems, whichinclude events that may be considered security issues and any case related to computer security, asan 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	4,517	3,684	4,865	13,066	13,831
Number of Incident *3	2,883	2,087	2,459	7,429	8,386
Cases Coordinated *4	1,523	1,232	1,465	4,220	4,807

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

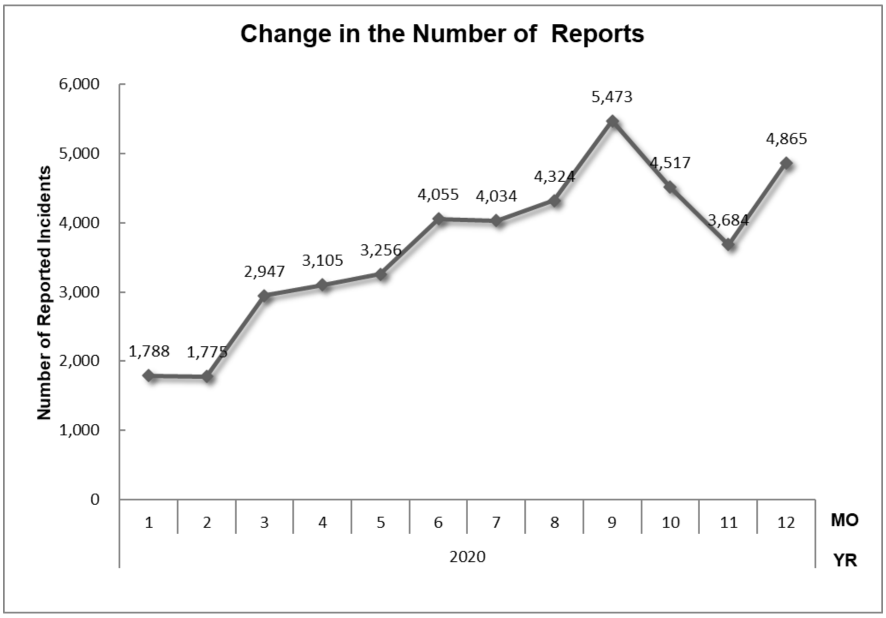
[*3] "Number of Incidents" refers to the number of incidents contained in each report. Multiple reports on the same incident are counted as 1 incident.

[*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.

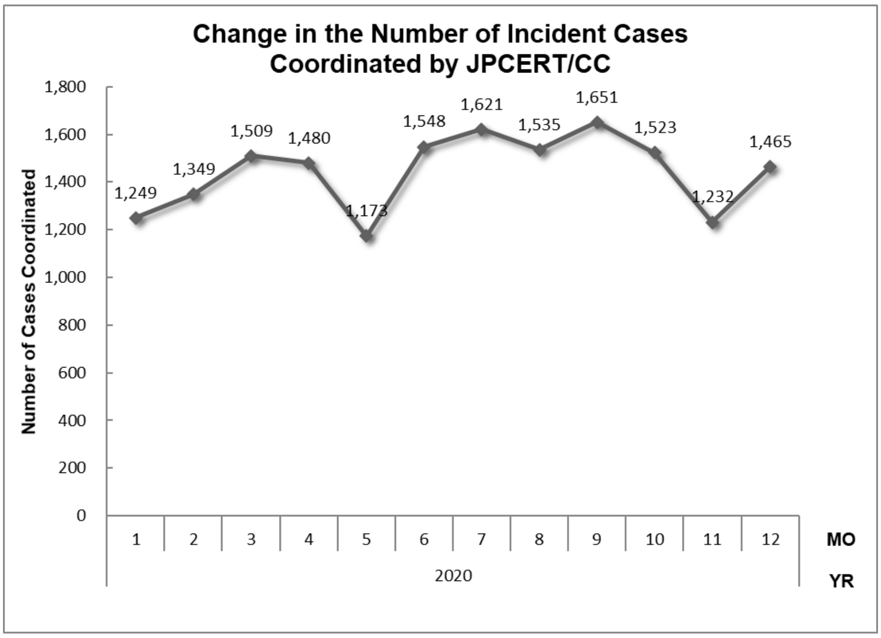
The total number of reports received in this quarter was 13,066. Of these, the number of domestic and overseas sites that JPCERT/CC coordinated with was 4,220. When compared with the previous quarter, the total number of reports decreased by 6%, and the number of cases coordinated decreased by 11%.

Year on year, the number of reports increased by 152%, and the number of cases coordinated increased by 20%.

[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]

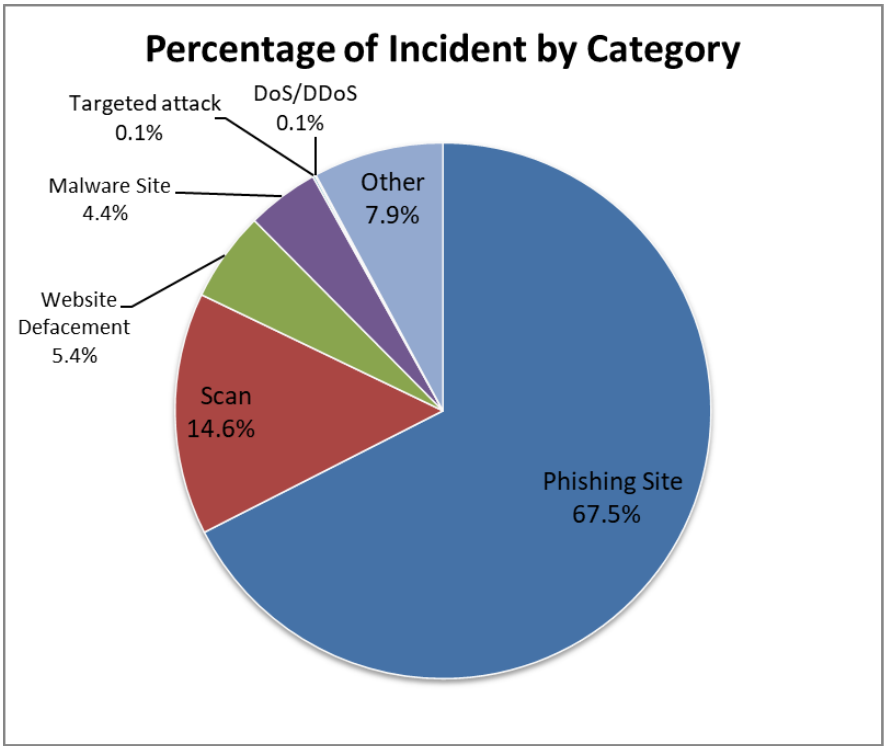


[Figure 2 : Change in the number of incident cases coordinated]

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]

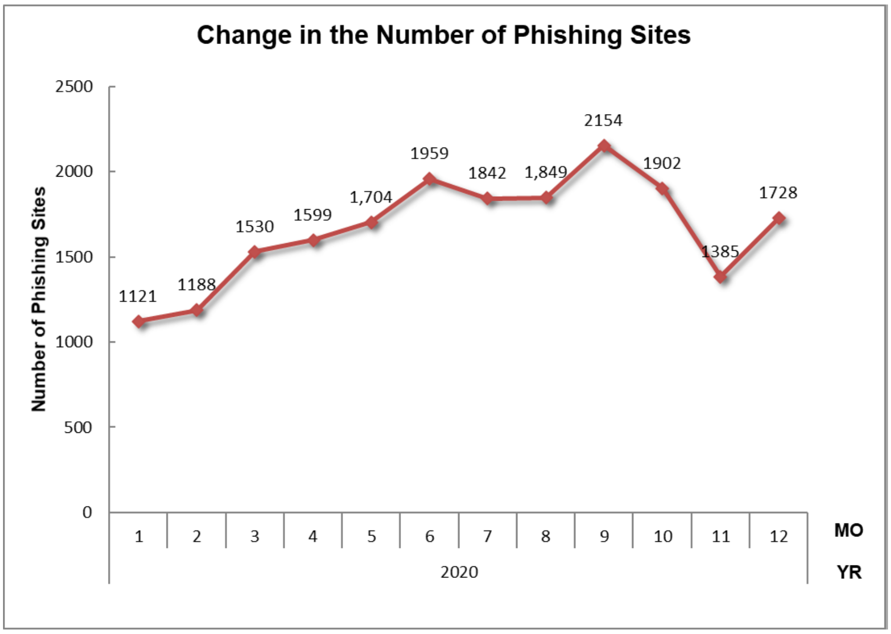
Incident Category	Oct	Nov	Dec	Total	Last Qtr.Total
Phishing Site	1,902	1,385	1,728	5,015	5,845
Website Defacement	198	135	71	404	374
Malware Site	82	143	99	324	158
Scan	381	312	393	1,086	1,380
DoS/DDoS	5	0	0	5	8
ICS Related	0	0	0	0	0
Targeted attack	7	3	0	10	16
Other	308	109	168	585	605



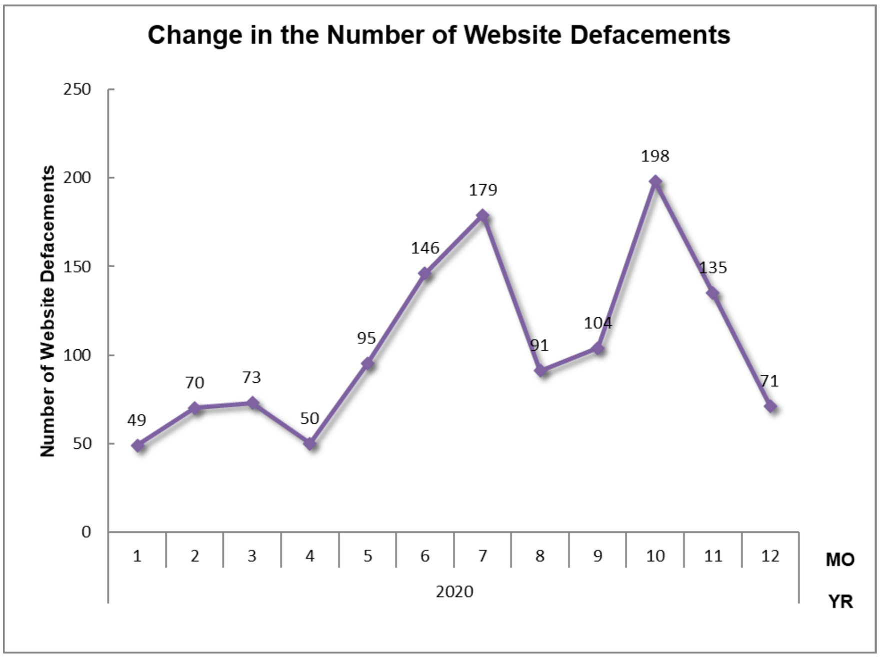
[Figure 3 : Percentage of incidents by category]

Incidents categorized as phishing sites accounted for 67.5%, and those categorized as scans, which search for vulnerabilities in systems, made up 14.6%.

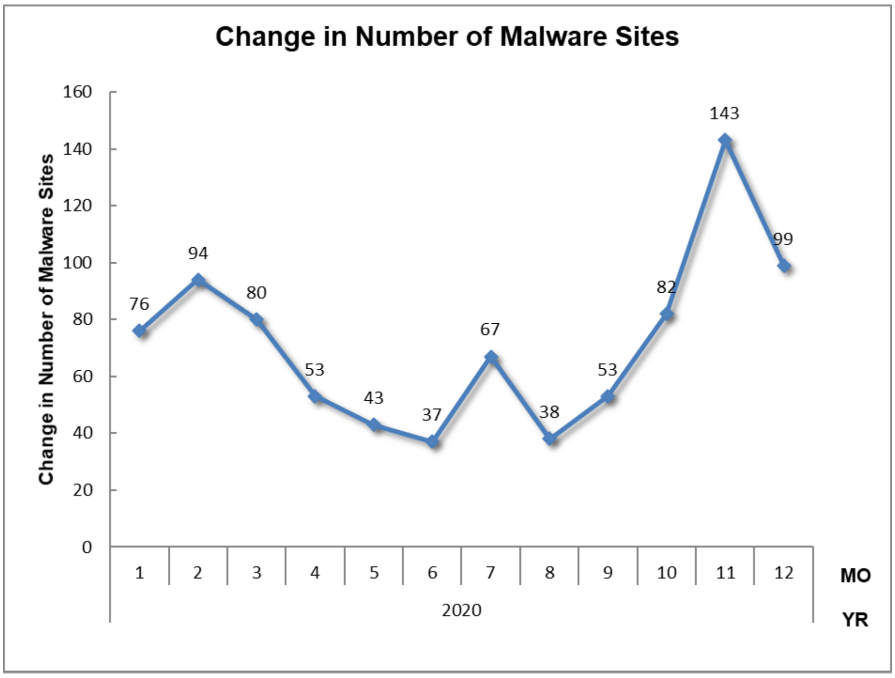
[Figure 4] through [Figure 7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



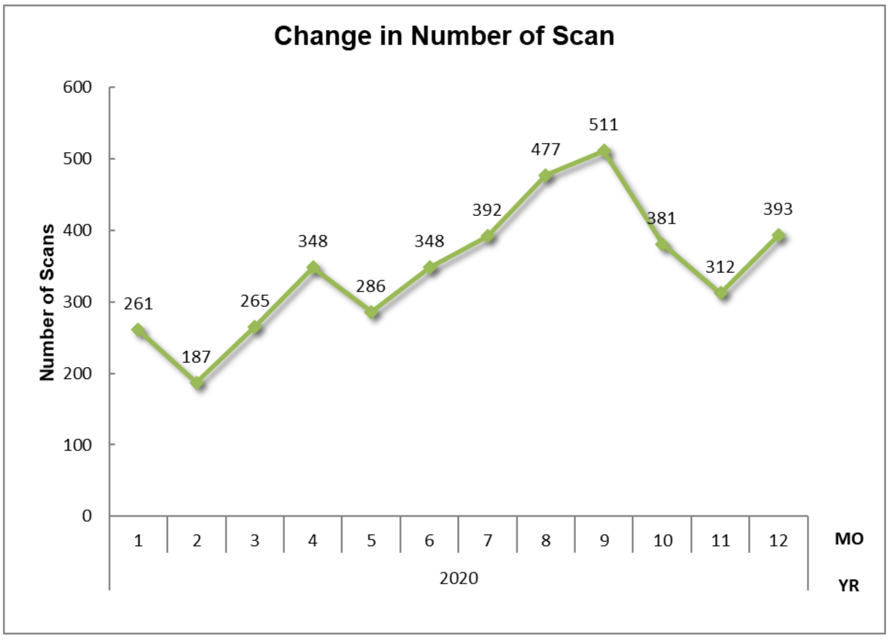
[Figure 4 : Change in the number of phishing sites]



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

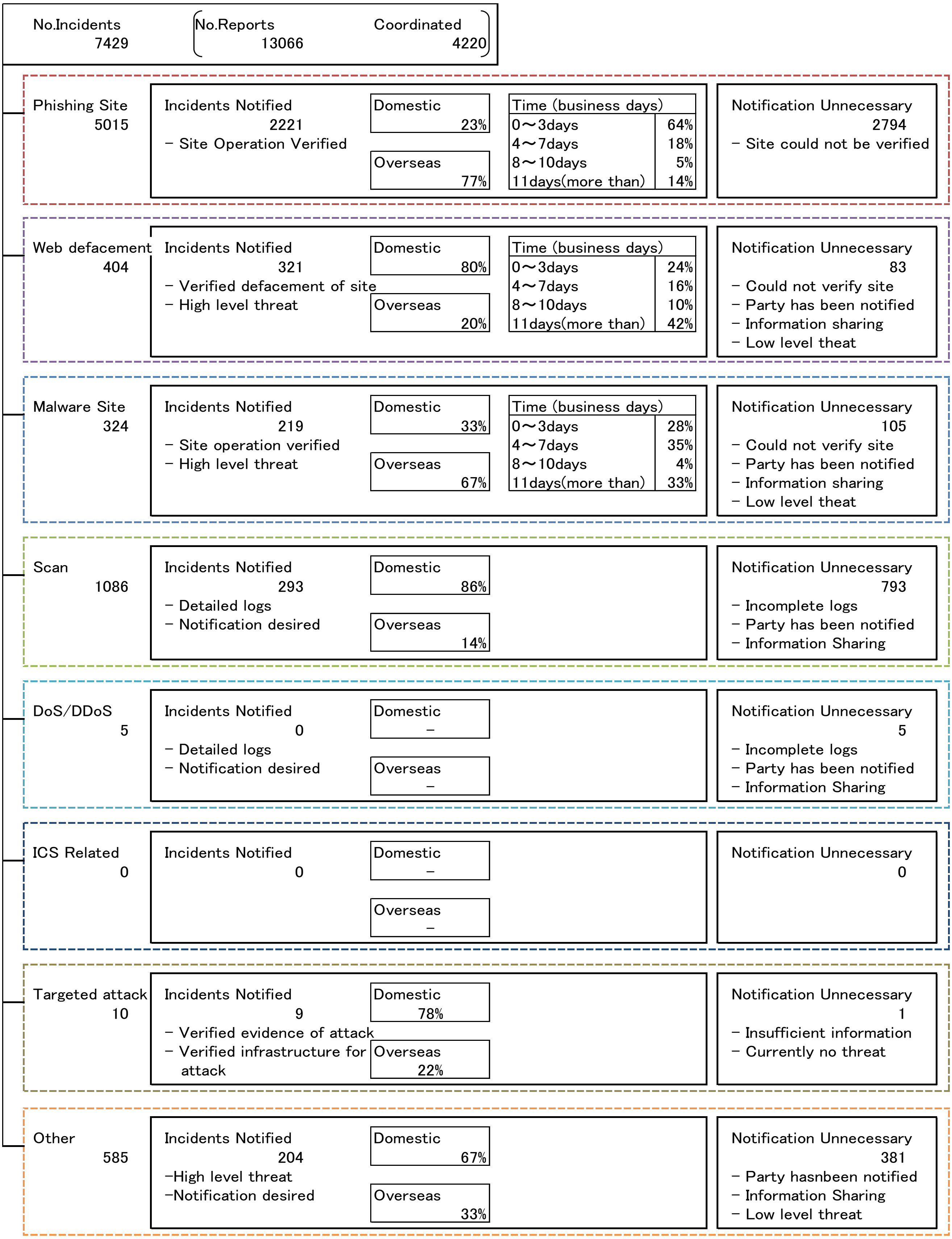


[Figure 6 : Change in the number of malware sites]



[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 7429 | No.Reports 13066 | Coordinated 4220

Phishing Site 5015

Incidents Notified 2221
- Site Operation Verified

Domestic 23%
Overseas 77%

Time (business days)	
0～3days	64%
4～7days	18%
8～10days	5%
11days(more than)	14%

Notification Unnecessary 2794
- Site could not be verified

Web defacement 404

Incidents Notified 321
- Verified defacement of site
- High level threat

Domestic 80%
Overseas 20%

Time (business days)	
0～3days	24%
4～7days	16%
8～10days	10%
11days(more than)	42%

Notification Unnecessary 83
- Could not verify site
- Party has been notified
- Information sharing
- Low level theat

Malware Site 324

Incidents Notified 219
- Site operation verified
- High level threat

Domestic 33%
Overseas 67%

Time (business days)	
0～3days	28%
4～7days	35%
8～10days	4%
11days(more than)	33%

Notification Unnecessary 105
- Could not verify site
- Party has been notified
- Information sharing
- Low level theat

Scan 1086

Incidents Notified 293
- Detailed logs
- Notification desired

Domestic 86%
Overseas 14%

Notification Unnecessary 793
- Incomplete logs
- Party has been notified
- Information Sharing

DoS/DDoS 5

Incidents Notified 0
- Detailed logs
- Notification desired

Domestic –
Overseas –

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

ICS Related 0

Incidents Notified 0

Domestic –
Overseas –

Notification Unnecessary 0

Targeted attack 10

Incidents Notified 9
- Verified evidence of attack
- Verified infrastructure for attack

Domestic 78%
Overseas 22%

Notification Unnecessary 1
- Insufficient information
- Currently no threat

Other 585

Incidents Notified 204
-High level threat
-Notification desired

Domestic 67%
Overseas 33%

Notification Unnecessary 381
- Party hasnbeen notified
- Information Sharing
- Low level threat

[Figure 8 : Breakdown of incidents coordinated/handled]

3. Incident Trends

3.1. Phishing Site Trends

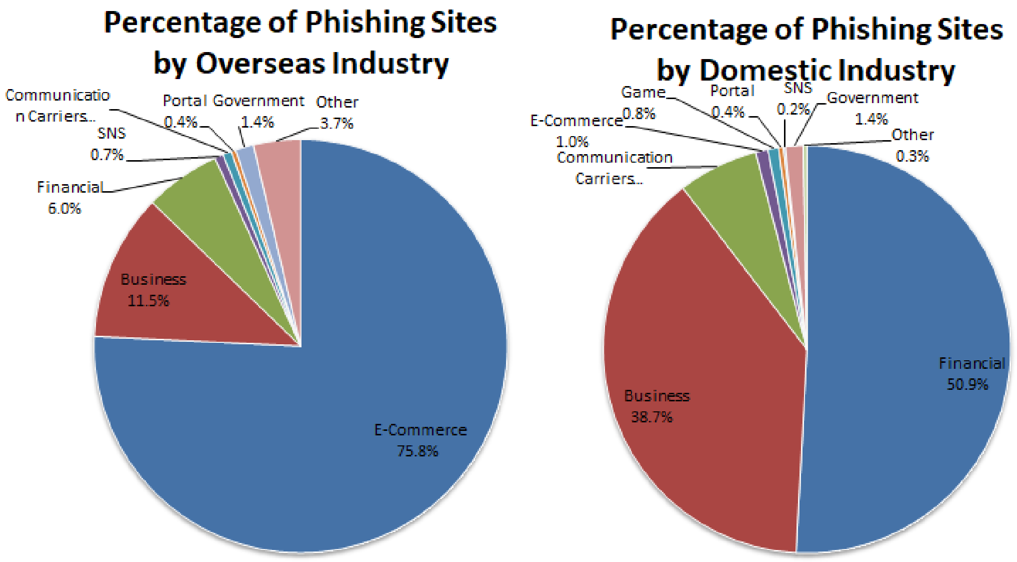
During this quarter, 5,015 reports on phishing sites were received, representing a 14% decrease from 5,845 in the previous quarter. This marks a 36% increase from the same quarter last year (3,700).

During this quarter, there were 2,635 phishing sites that spoofed domestic brands, increasing 29% from 2,043 in the previous quarter. And there were 1,629 phishing sites that spoofed overseas brands, decreasing 48% from 3,122 in the previous quarter. A 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	931	777	927	2,635(53%)
Overseas Brand	697	385	547	1,629(32%)
Unknown Brand [*5]	274	223	254	751(15%)
Monthly Total	1,902	1,385	1,728	5,015

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



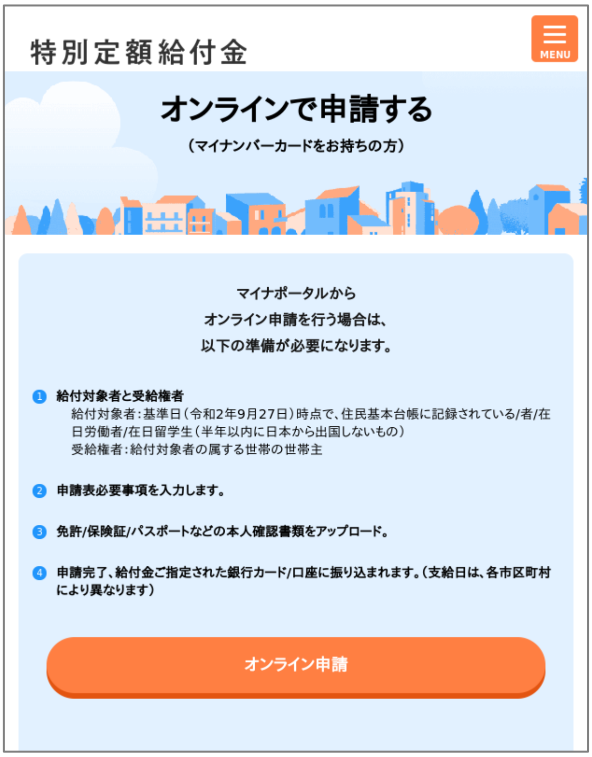
[Figure 9 : Percentage of reported phishing sites by industry (domestic/overseas)]

Out of the total number of phishing sites reported to JPCERT/CC, 75.8% spoofed e-commerce websites for overseas brands and 50.9% spoofed financial institution websites for domestic brands, both representing the largest share respectively.

As in the previous quarter, there were many phishing sites spoofing specific online shopping websites overseas, and in Japan the number of phishing sites spoofing financial institution websites has been increasing rapidly.

This quarter, JPCERT/CC received many reports of phishing sites offering special cash payment as a measure against the spread of COVID-19. According to these reports, attackers send an e-mail attempting to lure the recipient to a phishing site with information that a special website for special cash payment has been opened. Once the recipient accesses the phishing site, they are asked to enter their personal information and credit card information and upload a copy of a personal identification document such as a driver's license or passport.

These phishing sites have URLs that contain character strings like "kyufukin.soumu.go.jp" and "soumu-go-jp" to make them look like a website of the Ministry of Internal Affairs and Communications. At a glance, many of them are hard to identify as fake.



特別定額給付金

オンラインで申請する

（マイナンバーカードをお持ちの方）

マイナポータルから
オンライン申請を行う場合は、
以下の準備が必要になります。

1 給付対象者と受給権者
給付対象者：基準日（令和2年9月27日）時点で、住民基本台帳に記録されている/者/在日労働者/在日留学生（半年以内に日本から出国しないもの）
受給権者：給付対象者の属する世帯の世帯主

2 申請表必要事項を入力します。

3 免許/保険証/パスポートなどの本人確認書類をアップロード。

4 申請完了、給付金ご指定された銀行カード/口座に振り込まれます。（支給日は、各市区町村により異なります）

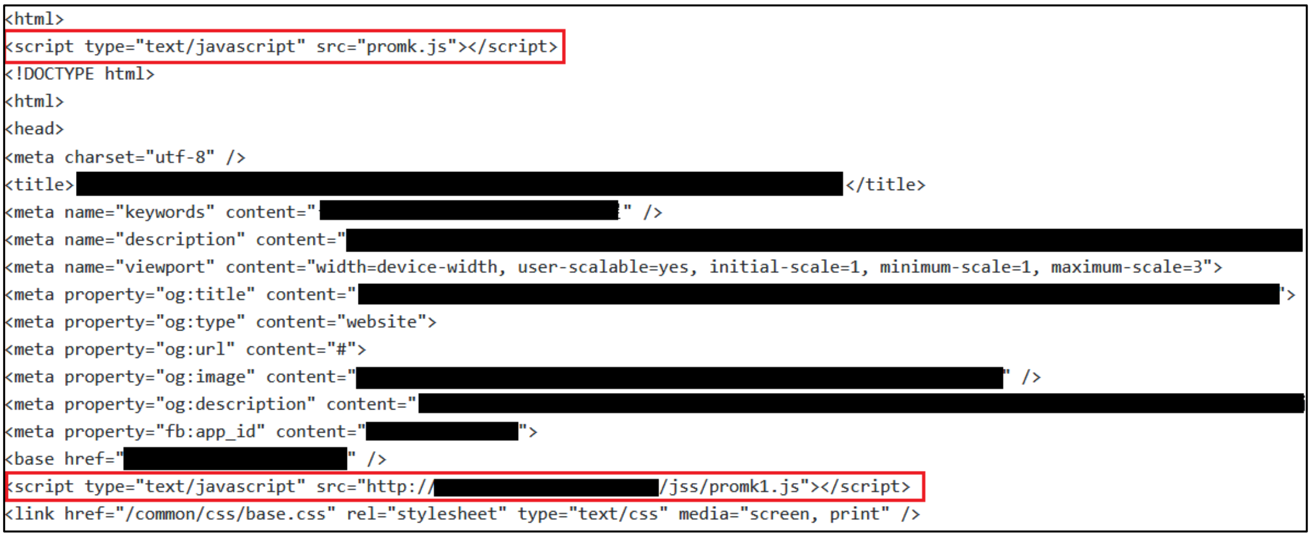
[Figure 10 : A phishing site offering special cash payment]

The parties that JPCERT/CC contacted for coordination of phishing sites were 23% domestic and 77% overseas for this quarter, indicating an increase in the proportion of overseas parties compared to the previous quarter (domestic: 29%, overseas: 71%).

3.2. Website Defacement Trends

The number of website defacements reported in this quarter was 404. This was an 8% increase from 374 in the previous quarter.

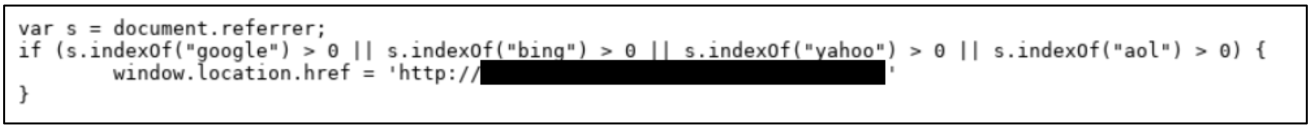
During this quarter, JPCERT/CC received multiple reports of being redirected from compromised websites to e-commerce websites that sell products of specific brands. The compromised websites were planted with a malicious JavaScript file designed to be loaded in a browser with script tags as shown in [Figure 11].



```
<html>
<script type="text/javascript" src="promk.js"></script>
<!DOCTYPE html>
<html>
<head>
<meta charset="utf-8" />
<title>[redacted]</title>
<meta name="keywords" content="[redacted]" />
<meta name="description" content="[redacted]
<meta name="viewport" content="width=device-width, user-scalable=yes, initial-scale=1, minimum-scale=1, maximum-scale=3">
<meta property="og:title" content="[redacted]">
<meta property="og:type" content="website">
<meta property="og:url" content="#">
<meta property="og:image" content="[redacted]" />
<meta property="og:description" content="[redacted]
<meta property="fb:app_id" content="[redacted]">
<base href="[redacted]" />
<script type="text/javascript" src="http://[redacted]/jss/promk1.js"></script>
<link href="/common/css/base.css" rel="stylesheet" type="text/css" media="screen, print" />
```

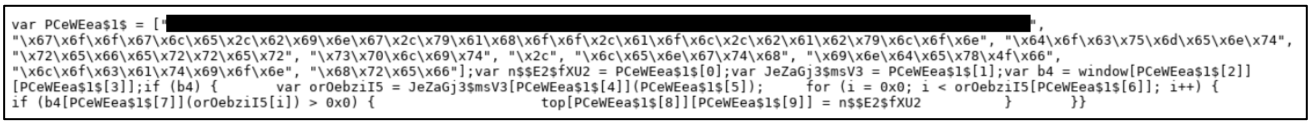
[Figure 11 : A page embedded with a malicious JavaScript file]

Examples of embedded malicious JavaScript files are shown in [Figure 12], [Figure 13] and [Figure 14]. Although these look different as they use different JavaScript obfuscation algorithms, they all check the referrer value and redirect the visitor to an e-commerce website only when accessed from a search engine.



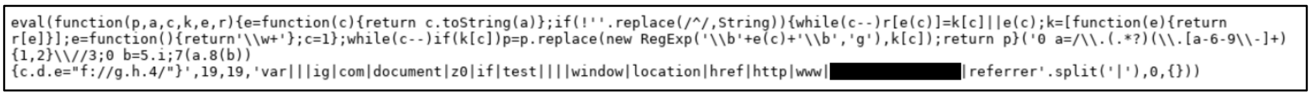
```
var s = document.referrer;
if (s.indexOf("google") > 0 || s.indexOf("bing") > 0 || s.indexOf("yahoo") > 0 || s.indexOf("aol") > 0) {
        window.location.href = 'http://[redacted]'
}
```

[Figure 12 : Example of a malicious JavaScript file 1]



```
var PCeWEea$1$ = ["[redacted]",
"\x67\x6f\x6f\x67\x6c\x65\x2c\x62\x69\x6e\x67\x2c\x79\x61\x68\x6f\x6f\x2c\x61\x6f\x6c\x2c\x62\x61\x62\x79\x6c\x6f\x6e", "\x64\x6f\x63\x75\x6d\x65\x6e\x74",
"\x72\x65\x66\x65\x72\x72\x65\x72", "\x73\x70\x6c\x69\x74", "\x2c", "\x6c\x65\x6e\x67\x74\x68", "\x69\x6e\x64\x65\x78\x4f\x66",
"\x6c\x6f\x63\x61\x74\x69\x6f\x6e", "\x68\x72\x65\x66"];var n$$E2$fXU2 = PCeWEea$1$[0];var JeZaGj3$msV3 = PCeWEea$1$[1];var b4 = window[PCeWEea$1$[2]]
[PCeWEea$1$[3]];if (b4) {        var orOebziI5 = JeZaGj3$msV3[PCeWEea$1$[4]](PCeWEea$1$[5]);      for (i = 0x0; i < orOebziI5[PCeWEea$1$[6]]; i++) {
if (b4[PCeWEea$1$[7]](orOebziI5[i]) > 0x0) {                        top[PCeWEea$1$[8]][PCeWEea$1$[9]] = n$$E2$fXU2            }        }}
```

[Figure 13 : Example of a malicious JavaScript file 2]



```
eval(function(p,a,c,k,e,r){e=function(c){return c.toString(a)};if(!''.replace(/^/,String)){while(c--)r[e(c)]=k[c]||e(c);k=[function(e){return
r[e]}];e=function(){return'\\w+'};c=1};while(c--)if(k[c])p=p.replace(new RegExp('\\b'+e(c)+'\\b','g'),k[c]);return p}('0 a=/\\.(.*?)(\\.[a-6-9\\-]+)
{1,2}\\//3;0 b=5.i;7(a.8(b))
{c.d.e="f://g.h.4/"}',19,19,'var|||ig|com|document|z0|if|test|||window|location|href|http|www|[redacted]|referrer'.split('|'),0,{}))
```

[Figure 14 : Example of a malicious JavaScript file 3]

3.3. Targeted Attack Trends

There were 10 incidents categorized as a targeted attack. This was a 38% decrease from 16 in the previous quarter. The incidents identified are described below.

(1) Lazarus Group attacks

During this quarter, JPCERT/CC continued to receive reports of targeted attacks aimed at organizations in Japan by a group called Lazarus (also known as Hidden Cobra). Confirmed attacks had sent malicious links intended to cause malware infections targeting individuals who belong to the target organizations via social media. Apparently, attackers are trying to infiltrate the internal network without being noticed by the target organization. They gain entry via social media used by individuals, instead of directly attacking the network.

The malware used by Lazarus is discussed in detail on JPCERT/CC Eyes.

Malware Used by Lazarus after Network Intrusion
https://blogs.jpcert.or.jp/en/2020/08/Lazarus-malware.html

BLINDINGCAN - Malware Used by Lazarus -
https://blogs.jpcert.or.jp/en/2020/09/BLINDINGCAN.html

(2) Attacks exploiting vulnerabilities in SSL-VPN products

Among the targeted attacks reported during this quarter, there were some cases in which vulnerabilities in SSL-VPN products were exploited to infiltrate networks. Attackers used new type of malware called SigLoader(1) to carry out attacks via vulnerabilities in SSL-VPN products installed at overseas offices of Japanese organizations.

Since 2019, various vulnerabilities in SSL-VPN products have been published, and attacks that target them continue to be carried out frequently. These vulnerabilities are exploited not just in targeted attacks but also in financially motivated ransomware attacks, and this trend will likely continue. Users of these products are encouraged to conduct thorough patch management and check logs regularly.

Past cases of attacks targeting vulnerabilities in Pulse Connect Secure are discussed in detail on JPCERT/CC Eyes.

Attacks Exploiting Vulnerabilities in Pulse Connect Secure
https://blogs.jpcert.or.jp/en/2020/04/attacks-exploiting-vulnerabilities-in-pulse-connect-secure.html

3.4. Other Incident Trends

The number of malware sites reported in this quarter was 324. This was a 105% increase from 158 in the previous quarter.

The number of scans reported in this quarter was 1,086. This was a 21% decrease from 1,380 in the previous quarter. The ports that the scans targeted are listed in [Chart 4]. Ports targeted frequently were SSH (22/TCP), SMTP (25/TCP) and HTTP (80/TCP).

[Chart 4 : Number of scans by port]

Port	Octl	Nov	Dec	Total
22/tcp	143	134	145	422
25/tcp	96	68	42	206
80/tcp	62	37	88	187
143/tcp	17	24	38	79
23/tcp	23	11	10	44
62223/tcp	16	15	12	43
445/tcp	8	13	20	41
443/tcp	1	10	29	40
5555/tcp	18	2	0	20
37215/tcp	2	6	6	14
3389/tcp	4	2	6	12
1433/tcp	2	2	8	12
8080/tcp	4	2	5	11
26/tcp	2	0	9	11
8081/tcp	1	1	4	6
2323/tcp	1	0	4	5
5500/tcp	0	2	2	4
81/tcp	1	2	0	3
3306/tcp	1	1	1	3

Unknown	8	13	18	39
Monthly Total	410	345	447	1202

There were 585 incidents categorized as other. This was a 3% decrease from 605 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 hosts impacted by a vulnerability in an SSL-VPN function of Fortinet's FortiOS

In the middle of November 2020, JPCERT/CC confirmed that a list of hosts impacted by a vulnerability in FortiOS that allows an unauthenticated attacker to download files (CVE-2018-13379) was published on forums and elsewhere. In addition to the hosts' IP addresses, this list contained account names and plaintext passwords needed to use SSL-VPN connections.

Based on this information, JPCERT/CC contacted operators managing the relevant IP addresses in Japan and asked them to change account passwords, introduce factor authentication, check the version of the devices they were using, and to perform an upgrade and take any other necessary steps if they were using a vulnerable version.

JPCERT/CC also issued a security alert regarding this matter.

Information disclosure concerning hosts impacted by a vulnerability in an SSL-VPN function of Fortinet's FortiOS (CVE-2018-13379)
https://www.jpcert.or.jp/newsflash/2020112701.html

(2) Coordination involving reports of IcedID malware

During this quarter, there were multiple reports of spoofed e-mail intended to cause infection with IcedID malware. This spoofed e-mail has the following characteristics, which closely resemble the methods used by Emotet to spread infections.

- The e-mail's body text is written in Japanese
- The e-mail is made to look like a reply to a past e-mail
- A password-protected ZIP file is attached
- The ZIP file contains a Word document that includes a macro (the recipient becomes infected with malware by enabling the macro)

JPCERT/CC issued a security alert via social media and requested the owners of the spoofed e-mail accounts to check if their accounts have been abused and change their passwords.

Twitter: Analysis Center (@jpcert_ac) (Japanese)
https://twitter.com/jpcert_ac/status/1324561915738091522

5. References

(1) LAC Co., Ltd.
[Urgent Report] LAC identified targeted attacks using SigLoader malware, which exploits Microsoft's digital signature files
https://www.lac.co.jp/lacwatch/report/20201201_002363.html

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 2020 Fiscal Year".

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