J-CSIP
Initiative for Cyber Security
Information sharing Partnership of Japan

Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP)

Annual Activity Report FY2012

IPA
IT SECURITY CENTER (ISEC)
INFORMATION-TECHNOLOGY PROMOTION AGENCY, JAPAN

Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP)

Annual Activity Report FY2012

Contents

Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP)

Annual Activity Report for FY2012

April 17, 2013
Information-technology Promotion Agency (IPA), Japan
IT Security Center

Summary

This document reports about the Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP, pronounced as JAY-sip)[1] operated by IPA, including its foundation, a summary of its activities and achievements for FY2012 (April 2012 ~ March 2013).

Terms in This Report

Terms	Description
Cyber Attack	In this report, the term is defined as the overall attacks conducted via the Internet including, but not limited to, unauthorized access, DoS/DDoS (Denial of Service) attack and targeted cyber attack.
Targeted Cyber Attack	In this report, the term is defined as a cyber attack that aims to steal information or execute other malicious intents directed at only small numbers of targets or many but limited scopes of targets. Measures against these attacks are introduced in the “Design and Operational Guide to Protect against ’Advanced Persistent Threats’” by IPA[2].
Virus	Computer virus. There are various categories (terms) out there, such as remote control virus or bot virus that enables an attacker to control an infected computer remotely, spyware that is mainly intended to steal information, or malware which generally means malicious programs. In this report, all of these are generally defined as virus.
Targeted Attack e-mail	In this report, the term is defined as virus email that is sent to specific organizations in order to steal information or execute other malicious intents. It has its characteristics, such as impersonating a sender who seems to be involved with a recipient, well-crafted mail subject and content that make the recipient open the attachment, and utilizing virus that cannot be easily detected by anti-virus software. When one receives a suspicious email, it is difficult to clearly distinguish whether the email he/she received is a targeted attack email or virus-attached spam email that is sent to wide range of people, and there are no criteria. Thus, a judgment needs to be comprehensively made based on various factors.

[1] J-CSIP：Initiative for Cyber Security Information sharing Partnership of Japan (IPA)
http://www.ipa.go.jp/security/J-CSIP/index.html (in Japanese only)

[2] “Design and Operational Guide to take measure against ‘Advanced Persistent Threats’ (IPA)
http://www.ipa.go.jp/files/000017299.pdf

1 Overview of J-CSIP

1.1 Background of Foundation

Cyber attacks that target intellectual property and critical infrastructure, or disclosure of classified information are frequently occurring around the world. Targets that need to be protected by securing IT have qualitatively shifted to those in the areas directly related to people's lives and economic activities. Under such circumstances, the ”Study Group on Cyber Security and Economy” was launched by the Ministry of Economy, Trade, and Industry (METI) with participating experts in December 2010[3] and several meetings were held.

The “measures against targeted attacks” were suggested as the main conclusion and recommendations in the interim report of this study group[4]. As one of its effective measures, the necessity of information sharing among the organizations was discussed by the group. Also, in 2011, at the same time as the group was writing up the interim report, various cyber incidents that seemed to have resulted from targeted cyber attacks occurred in Japan.

After such incidents, the representatives of nine critical manufacturing vendors (heavy industry and heavy electrical industry) had gathered under the request of METI on October 25, 2011 and the Minister requested for strengthening security. The Initiative for Cyber Security Information sharing Partnership of Japan (J-CSIP) was founded as a countermeasure against targeted cyber attacks and cooperative public-private information sharing system.

Significance of Information Sharing

To take effective measures against cyber attacks, it is important to know the threats against own organization and information about real incidents. On the other hand, it is hard to identify and detect the attacks that are conducted against small numbers of targets or many but limited scopes of targets. Even if an attack is detected, there are not many opportunities or it is difficult for the attacked organization to share the information with other organizations. Thus, it is almost impossible to understand the real situation.

In the ”Study Group on Cyber Security and Economy” meetings, there were opinions that government should take lead to clear various obstacles regarding information sharing, such as:

- Need for discussion of scheme, anonymization process of information source and sensitive information
- Need for developing a closed, effective information sharing community where members could utilize sensitive information

Additionally, it is effective to share information among organizations in the same industry in a situation where an attacker conducts targeted cyber attacks against a specific industry. However, these organizations are the competitors.

Cyber attacks and countermeasures are asymmetrical, which means attackers have more advantage over defenders. Under the common understanding that it is critical for the defenders to share attack information, the J-CSIP members accept each other’s various limitations and work together on information sharing as one of the countermeasures.

[3] ”The Study Group on Cyber Security and Economy” (METI)
http://www.meti.go.jp/committee/kenkyukai/mono_info_service.html#cyber_security (in Japanese)

[4] Publicity of interim report, “Study Group on Cyber Security and Economy” (METI)
http://www.meti.go.jp/english/press/2011/0805_04.html

1.2 Purpose of J-CSIP

J-CSIP is an effort to promote information sharing among member companies through a public organization, IPA, as an information hub (aggregation center) and fight sophisticated cyber attacks utilizing shared information.

IPA collects information on cyber attacks that are detected at member companies and their group companies under the NDA[5] signed between IPA and each member company (or industry organization). IPA anonymizes the information source (the member company who provided the information), obscures or deletes sensitive information, adds an analysis result by IPA, makes the information sharable with the authorization from the information source, and shares the information with member companies (Figure 1).

Through information sharing, J-CSIP aims to enable the following and enhance the defense against cyber attacks at each member and industry.

1. Early detection of similar attacks and avoidance of the damage
2. Implementation of defense against attack
3. Planning the countermeasures for future attacks

Currently, J-CSIP focuses on the targeted cyber attack emails, which are a major threat frequently used in cyber attacks these days.

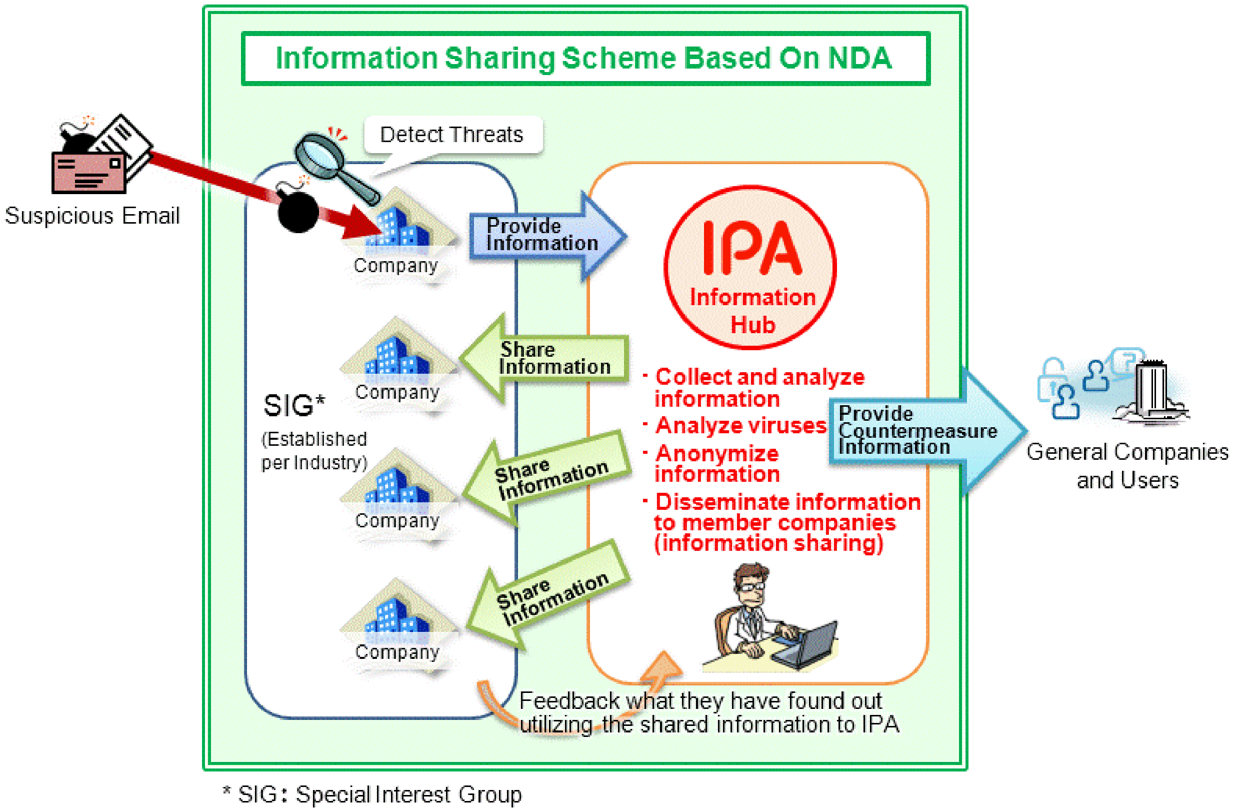
Information Sharing Scheme Based On NDA
Suspicious Email
Detect Threats
Company
Provide Information
IPA
Information Hub
Share Information
Company
SIG*
(Established per Industry)
Share Information
Company
Share Information
Company
· Collect and analyze information
· Analyze viruses
· Anonymize information
· Disseminate information to member companies (information sharing)
Provide Countermeasure Information
General Companies and Users
Feedback what they have found out utilizing the shared information to IPA
* SIG: Special Interest Group

Figure 1 J-CSIP Information Sharing Activity Based on NDA

[5] NDA: Non-Disclosure Agreement

2 Achievements

The following two are main achievements of J-CSIP for FY2012.

- Establishment of the information sharing scheme **among 39 organizations across 5 industries**
- Sharing of **160 cases** (between April 1, 2012 and March 31, 2013), and confirmation of qualitative effectiveness of information sharing

2.1 Establishment of Information Sharing Scheme

Table 1 shows the history of development and expansion of the J-CSIP information sharing scheme including the background of foundation.

Table 1 Development of J-CSIP

No.	Time	Contents
1	Dec. 2010 ~	The "Study Group on Cyber Security and Economy" launched
2	Aug. 2011	The "Study Group on Cyber Security and Economy" interim report (proposal of necessity of information sharing) submitted The "Pilot Project on Information Sharing Scheme for Targeted Attacks"[6] launched
3	Sep. ~ Oct. 2011	Multiple serious incidents that seemed to have resulted from targeted cyber attacks in japan were reported by media
4	Oct. 25, 2011	J-CSIP founded
5	~ End of Mar. 2012	NDA and information sharing rules were developed through the discussions among METI, IPA and nine critical manufacturing vendors
6	Apr. 2012	NDA was signed with the Critical Manufacturing SIG members and the SIG came into operation
7	Jul. ~ Oct. 2012	The Electric Power SIG, Gas SIG, Chemical SIG and Petroleum SIG were founded and came into operation. The number of J-CSIP members became 38 (1 organization added afterward)
8	Oct. 2012	Introduced information sharing among the SIGs (among industries)
9	~ As of Apr. 2013	Continuing information sharing activity

First, J-CSIP started to prepare for launching its activity between IPA and the working-level representatives of the SIG (Special Interest Group[7]) for nine critical manufacturing venders[8]. The followings were the main issues discussed at the meetings.

- Structure and contents of NDA
- Procedure and rules for information sharing
  - Rules for information handling and flow of information sharing (operational flow)

[6] A research project on the rules and implementation methods to develop an "information sharing scheme". As part of the project, the "Workshop for Sharing Cyber Information" was held.
http://www.jpcert.or.jp/event/CTAPP.html (in Japanese)

[7] It means an "information sharing group for a specific area of interest (cyber attack information specific to each industry)". In J-CSIP, a SIG is a collective body of participating member companies for each industry.

[8] Besides the METI, IPA and nine critical manufacturing vendors, Japan Computer Emergency Response Team Coordination Center (JPCERT/CC), Japan Users Association of Information Systems (JUAS) and LAC Co., Ltd. joined the discussions.

- Method of providing and receiving specific information and point of contact
- Standard and method for information anonymization, format and describing method for providing and sharing of inform

- Information exchange of the measures against cyber attacks at each member company

Through these discussions, NDA was signed between IPA and each company, the rules for information sharing were established and J-CSIP launched its full-fledged information sharing activity in April 2012.

From July to October 2012, a SIG was founded for each of the electric power, gas, chemical and petroleum industry following the same SIG scheme as the Critical Manufacturing SIG and came into operation. Since October 2012, in addition to information sharing within each SIG, information sharing among the SIGs (among industries) started. As of April 2013, the number of member companies is 39 across 5 SIGs.

With the authorization from information source, depending upon the needs, J-CSIP provides part of the provided information to information security organizations, such as JPCERT/CC, to cooperate and coordinate countermeasures. Additionally, when a serious incident occurs, J-CSIP is to collaborate with METI and NISC (National Information Security Center) as well (Figure 2).

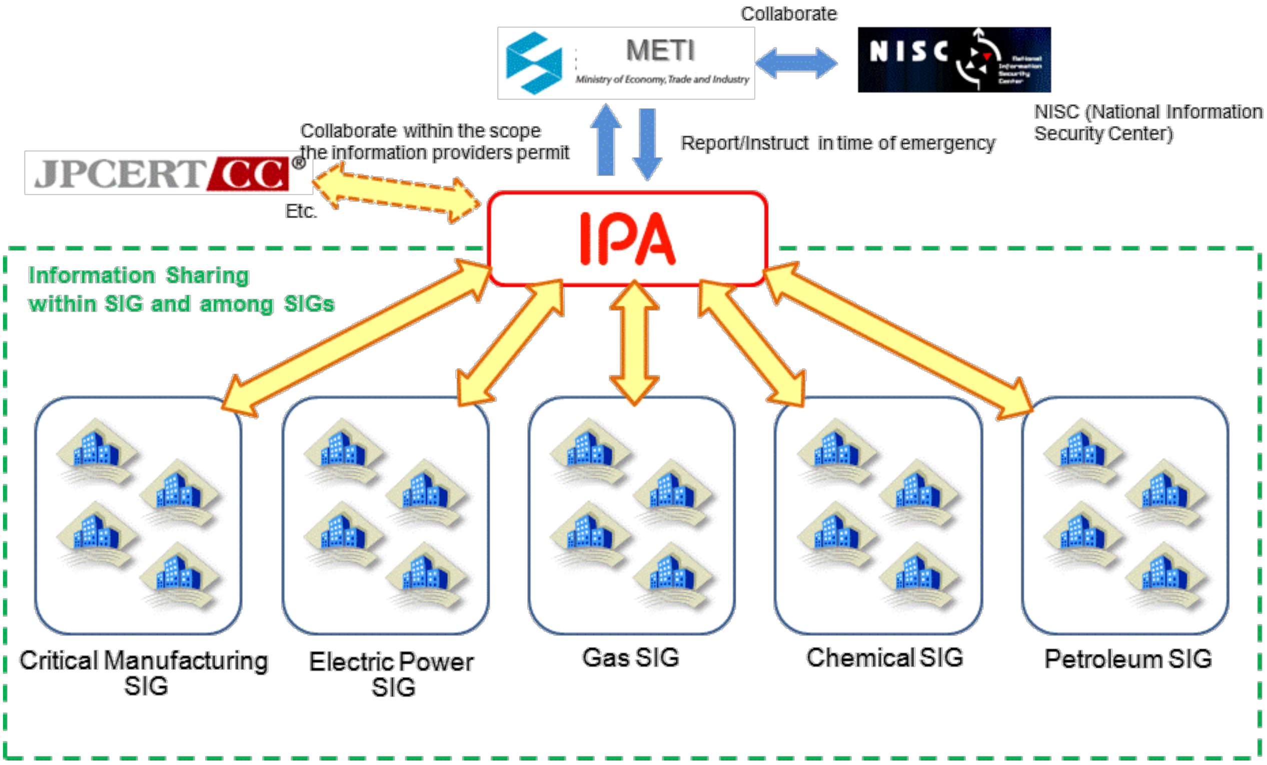
Collaborate
METI
Ministry of Economy, Trade and Industry
NISC
NISC (National Information Security Center)
Collaborate within the scope the information providers permit
Report/Instruct in time of emergency
JPCERT/CC®
Etc.
IPA
Information Sharing within SIG and among SIGs
Critical Manufacturing SIG
Electric Power SIG
Gas SIG
Chemical SIG
Petroleum SIG

Figure 2 Information Sharing System Including Several SIGs and Relevant Organizations

2.2 Overview of the Achievements of Information Sharing

Having defined an information sharing scheme and rules that are based on NDA, J-CSIP has been able to collect and utilize a lot of attack information, including sharing of 160 attacks information in FY2012. At the same time, J-CSIP became capable of not only sharing information on individual attacks, but also identifying the trend and correlation among multiple attacks.

A new trial of information sharing among various companies in the same industry (who compete each other in the market) produced not only a quantitative effect on cyber defense, but also a qualitative effect as shown below in terms of attack detection, prevention and countermeasures. For this, J-CSIP was recognized as one of the effective countermeasures against cyber attacks.

- In the past, it was difficult for companies to learn about each other's situation regarding cyber attacks. But by implementing information sharing through a public organization (IPA) as an information hub, it became possible for them to learn that the same or similar attacks targeting their industry were truly happening, and detect and block attacks through cooperation.

- With the premise that information is handled under the NDA, it is possible for companies to make a prompt judgment on whether to share and what to share. As a result, the quality of information became high (in terms of freshness and density) and which made the information effective to detect and protect from attacks.

- It has also become possible for member companies to lean the trend or correlation of attacks due to the scheme where IPA acts as an information hub. Sharing these information has helped the companies to consider countermeasures to prepare for future expected attacks.

3 Results for FY2012

3.1 Attacks and Trends

Table 2 shows the number of suspicious emails that could be targeted attacks reported by the J-CSIP member companies to IPA, and the number of information disseminated by IPA to member companies based on the shared information (table 2).

Table 2 Reported and Shared Information

No	Subject	Number of Case (total of 39 organizations across 5 SIGs)
1	Number of information reported by member companies to IPA	**246 cases**
2	Number of information disseminated by IPA to member companies	**160 cases** *1

*1 There is the difference in the number of cases reported to IPA and disseminated by IPA since in some cases, multiple cases were counted and disseminated as 1 case when the same or almost identical targeted emails were reported, or in other cases, the information was not disseminated because it was concluded that the reported email was widely-sent spam emails.

IPA analyzed the reported suspicious emails and viruses attached to them, and made statistical data. As a result, the following trends were observed[9]. The detail of the statistical data is available in Annex.

- Majority of targeted emails were sent from South Korea as the top country, Japan as the second and the United States as the third. These three countries account for more than half of the total.
- The suspicious connecting IP addresses (C2 or other malicious servers) the virus tried to establish a connection with most belonged to the United States (accounted for nearly 30%) and the rest of others belonged to Asian countries. There were also Japanese IP addresses and they accounted for 7%.
- Nearly 80% of suspicious mails had an attachment file that might be virus. Approximately 10% of emails included URLs linked to suspicious websites.
- Among the attachment files, Office document files and .exe files had the almost same ratio and they accounted for over 90% of the total.

IPA will further call on the member companies to report incidents and provide information to J-CSIP, as IPA tries to improve its capability as an information hub.

In 2008, IPA opened a consultation service to provide information and consultation about targeted attacks[10] and has been asking public and private organizations and general users to report targeted email. After about 5 years, the accumulative number of the targeted emails reported is 145 at the end of FY2012. The knowledge acquired from the reported information is publicly released as "IPA Technical Watch[11]" or other media.

[9] The possibility of the attackers using other people`s computer to hide their identities needs to be considered with regard to the source IP addresses and suspicious connecting IP addresses.

[10] In 2008, it was called the "Suspicious Email 110". Currently, support is provided through the "Targeted Cyber Attack Special Consultation Desk" including consultation for various security matters.
http://www.ipa.go.jp/security/tokubetsu/ (in Japanese)

[11] IPA Technical Watch – Report Vol. 4 and Vol. 12 are about targeted attack emails.
http://www.ipa.go.jp/security/technicalwatch/ (in Japanese)

3.2 Case Study of Information Sharing

This is a case study of information sharing at J-CSIP. In this case, through information sharing, it was revealed that other member companies received the same types of suspicious emails as the reported member company. Those reports were aggregated and further shared with the members.

The case is divided into three phases and chronologically explained:

- Phase one：information sharing about a suspicious email
- Phase two：identifying the same type of emails at other member companies
- Phase three：information analysis and further information sharing

Figure 3 shows the flow from the detection of a suspicious email to information sharing through IPA at the phase one.

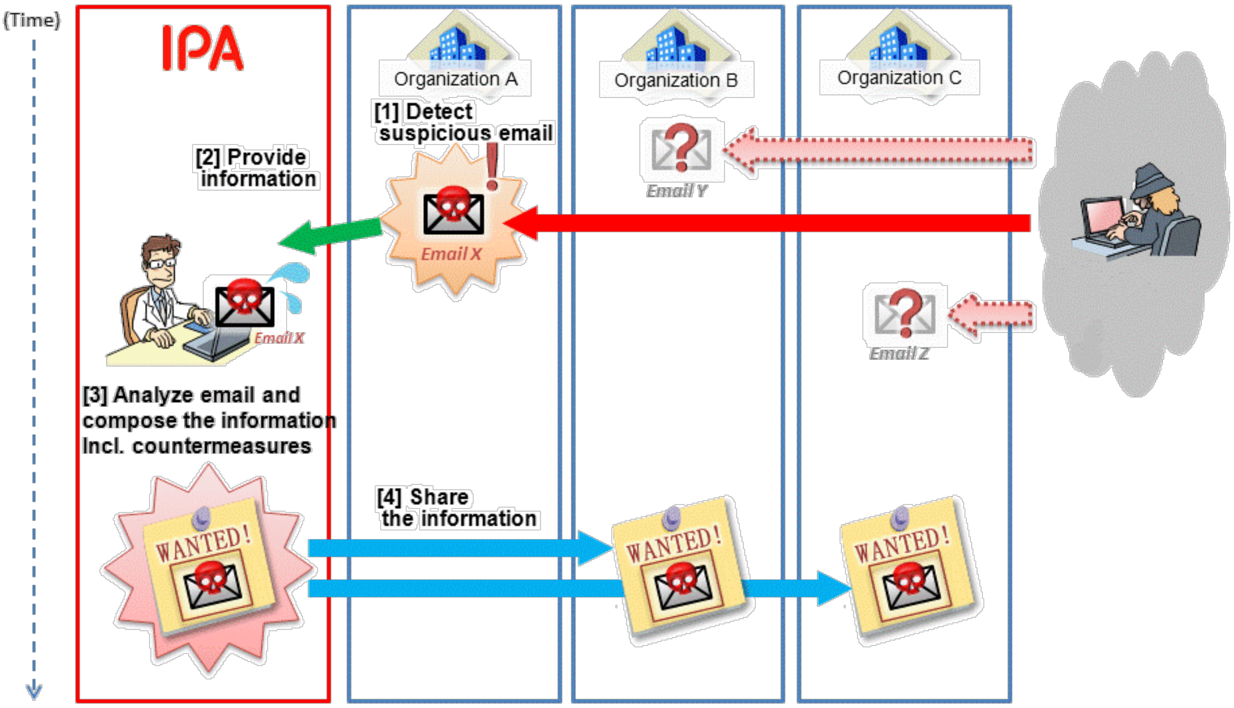
(Time)
IPA
Organization A
Organization B
Organization C
[1] Detect suspicious email
[2] Provide information
Email X
Email Y
Email Z
[3] Analyze email and compose the information Incl. countermeasures
[4] Share the information
WANTED!

Figure 3　Phase One: Sharing Information about Suspicious Email

[1] Detect a suspicious email ~ [2] Provide information

In this case, at first, a suspicious email was detected at a J-CSIP member, the organization A (Figure 3, [1]). The suspicious email was promptly provided by the organization A to IPA (Figure 3, [2]).

At this point, it was uncertain if other J-CSIP members had also received the same email (but it later turned out that they did receive). Here, we call the email sent to and reported by the organization A as ”Email X”, the ones sent to and reported by the organization B and C as “Email Y” and ”Email Z”, respectively.

[3] Analyze email and assemble information including countermeasures ~ [4] Share information

IPA analyzed the provided “Email X”, assembled the information to detect the same type of suspicious emails (Figure 3, [3]), acquired the permission from the information source (the organization A), and promptly shared information with other J-CSIP members (Figure 3, [4]).

Figure 4 shows the flow of finding and reporting the same types of suspicious emails at other organizations at the phase two.

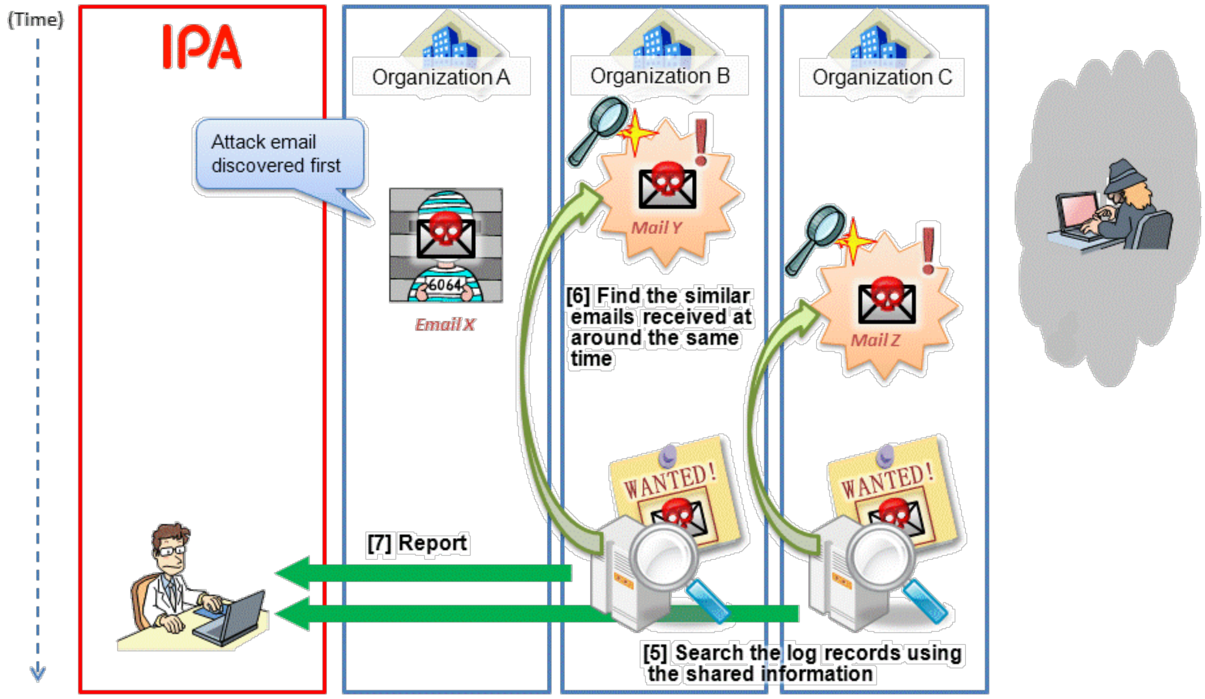
(Time)
IPA
Organization A
Organization B
Organization C
Attack email discovered first
6064
Email X
Mail Y
Mail Z
[6] Find the similar emails received at around the same time
WANTED!
WANTED!
[7] Report
[5] Search the log records using the shared information

Figure 4 Phase Two: Looking for the Same Types of Suspicious Emails at Each Organization

[5] Search log files based on the shared information

Based on the information shared in Figure 3 [4], each organization checked the log files of their mail server (Figure 4, [5]).

[6] Identify the same types of suspicious email received at around the same time period

As a result, the organization B, C and others found the same type of suspicious email “Email Y” and “Email Z”. These were received at around the same time as the “Email X” (Figure 4, [6]).

[7] Report

J-CSIP regularly calls on the members to report to IPA about what they have found out using the shared information as much as they could. Following this principle, the reports were made by the organization B and C regarding the discovery of the same type of suspicious emails (”Email Y” and ”Email Z”) (Figure 4, [7]).

Figure 5 shows the flow of further information sharing after collecting a series of attack information at the phase three.

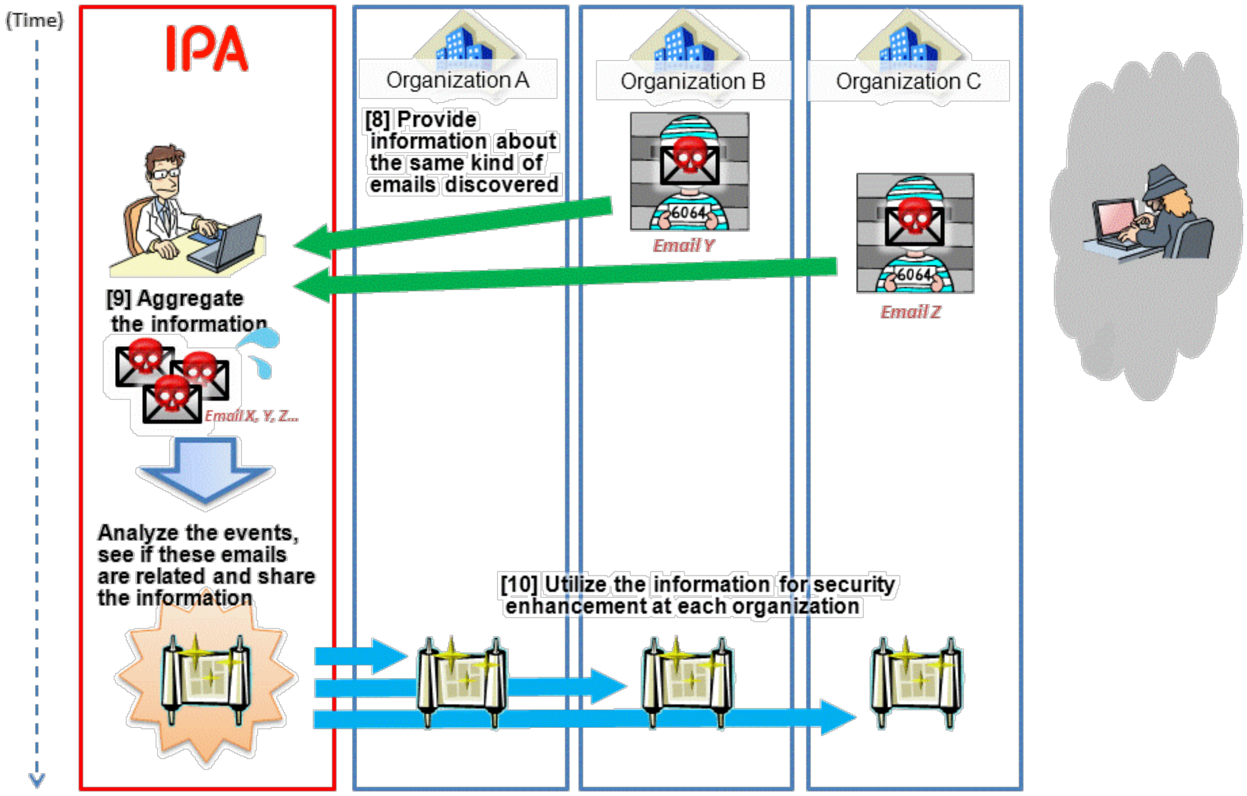
(Time)
IPA
Organization A
Organization B
Organization C
[8] Provide information about the same kind of emails discovered
6064
Email Y
6064
Email Z
[9] Aggregate the information
Email X, Y, Z...
Analyze the events, see if these emails are related and share the information
[10] Utilize the information for security enhancement at each organization

Figure 5　Phase Three: Collection and Analysis of Information and Further Information Sharing

[8] Provide information about the same types of suspicious emails

As IPA received the report on the Email X,Y and Z, IPA focused on the difference in the receiving time at each organization, things in common and the difference among those emails, and asked for more information as much as possible. The organization B and C answered the call and provided more information on the “Email Y” and “Email Z”, respectfully (Figure 5, [8]).

[9] Aggregate information, promote more information sharing ~ [10] Utilize for future efforts

IPA extracted the things in common and difference in individual emails and attachment files (virus) after aggregating the information. IPA analyzed possible connection among them, sorted the events chronologically, analyzed the attack techniques, and further shared the analysis result with the member companies (Figure 5, [9]). This information was utilized to consider the future countermeasures at each member companies (Figure 5, [10]).

3.3 Consideration

Here, we examine the case introduced in the section 3.2 from the three viewpoints that J-CSIP intends to achieve as declared in the section 1.2 of this report.

1. Early detection of similar attacks and avoidance of the damage

In this case study, other member organizations were able to identify the same type of attacks through sharing of the information on the attack email found at the organization A. This could be considered as a direct outcome of the successful information sharing.

It is not easy to thoroughly find or prevent attack emails. However, if an attack email is detected by even just one organization among various organizations who have received the same attack emails, the level of protection could be improved on the whole by sharing the information with others.

Beside this case study, there are other cases where information sharing resulted in discovering similar attacks or preventing attacks (e.g. blocking attack emails) in advance, which have made the member companies rate information sharing as effective.

2. Implementation of defense against attacks

J-CSIP shares the information when IPA or the information source analyzes and identifies the suspicious connecting IP addresses (C2 or other malicious servers) used by attachment files (viruses). This information is utilized for taking actions such as blocking outgoing access using proxy server or firewall. Even if attack emails weren't detected based on the shared information or another new attack occurs, if the virus tries to establish the same type of malicious connections to the suspicious connecting IP address previously identified, the damage can be mitigated.

In this case study, IPA confirmed and promptly shared all suspicious connecting IP addresses used by the virus and the information is used to strengthen security at each member company.

3. Planning the countermeasures for future attacks

In the case study, IPA analyzed the connection among the collected attack information, sorted the events and shared the analysis result with the member companies. For that, the member companies could understand the attack techniques and situations such as the flow of and the correlation among a series of attacks. This information could lead to formulating measures for possible future attacks, what kind of measures each company needs to take or how the current measures can be improved to more effective ones. This can be said that it is a characteristic achievement of the J-CSIP activity enabled by aggregating the information at the hub (IPA).

Conclusion – Importance of awareness of attacks and information sharing

In the case study, information sharing went very smoothly since each member company was used to the information sharing flow through the past activities and the organization A promptly managed to detect and provided the information. When we share the information, it is critical that the rules, procedures, and points of contact should be clearly defined, and getting used to the procedures by repetitive information exchange. The same thing could be said not only between organizations, but also within an organization.

Additionally, in the case study, some companies said "We confirmed receiving the same type of attack email on the mail server based on the shared information. But the recipient deleted the email without opening its attachment file. This event was not reported to the system administration department." This meant that there was no problem since no damage was caused, and it also meant that this organization was able to notice that there were attack emails they did receive but did not know about.

As a countermeasure against virus email for general users, IPA recommends that, fundamentally, the recipient delete a suspicious email without opening it. However, for an organization to take measures one step further, it is important for the organization to know what types of attack emails are sent to whom or which section of the organization. After that, it is necessary for the organization to evaluate how effective the current defense-in-depth security measures are and consider improvements.

The hearing from the member companies was done almost one year after the launch of J-CSIP. Some companies said that "We used to tell our employees to delete suspicious emails at once, but we changed our operational policy and now they are to report them to the system administration department." This change may put another burden on the system administration department, but it is an important and useful way to know if there are attacks against the organization and the reality if there are being attacked. Also, if a suspicious email is found, the organization can promptly investigate if other employees or departments have received the same type of suspicious emails. Then, by sharing information through J-CSIP, it leads to an effective improvement of defense against attacks for all members like the case study in section 3.2.

4 Future Plan

METI and IPA believe that the J-CSIP approach is effective to fight cyber attacks including targeted attacks. The J-CSIP member companies rate J-CSIP highly as well.

Working on broadening the members, expanding the information it shares and improving the overall efficiency, IPA will continue the J-CSIP effort and promote the better defense against cyber attacks including targeted attacks for individual and companies.

Request for Reporting Targeted Attacks to the "Targeted Cyberattack Special Consultation Desk"

IPA provides a consultation service for home users and companies/organizations and collects reports on cyber attack incidents in general including targeted attacks at the "Targeted Cyberattack Special Consultation Desk". To understand the techniques used and what is really going on with the targeted cyber attacks that are focusing on a very limited targets, reports from those who have received and detected such attack is absolutely imperative. Please call or email the Desk and share the information.

Targeted Cyberattack Special Consultation Desk (IPA)
http://www.ipa.go.jp/security/tokubetsu/

Annex: Statistics

The below shows the statistics about the viruses, such as suspicious emails and attachment files, reported to and examined by IPA. “N (the number of subjects)” is different for each data set. The reason is explained at the end of this report. Also, since the data values shown in the graphs are rounded off to the nearest whole number, the total may not be added up to 100.

1. Distribution of the Source IP Address of Suspicious Emails by Region

The regional distribution of the source IP address of the suspicious emails reported to IPA is shown in Figure 6[12]. A source IP address here means an IP address which we could guess from the email’s header information that the attacker has possibly used it to send the attack email.

According to the statistics, the 1st, 2nd and 3rd are Korea, Japan and the United States, respectfully, and these top three regions account for half of the total. After that, Hong Kong and China follow as the 4th and 5th. Malicious emails may be sent by the servers, PCs or VPN services that have been hijacked and exploited through remote control virus or unauthorized access by the attacker to conceal his or her identity. Thus, this data cannot be directly used for profiling the attacker, but it is distinctive that besides the U.S., ranked-in countries are concentrated in Asia.

The source IP address of one third of the emails submitted to IPA was unidentifiable because the header information was not ensured or the header contains no trace of the source IP address.

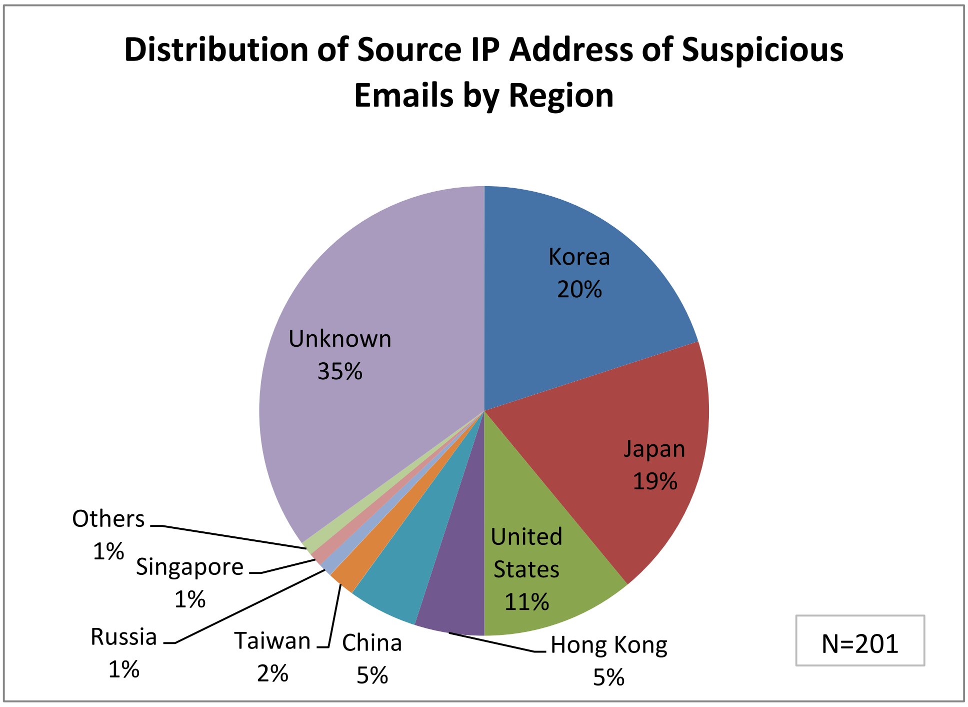

Figure 6 Distribution of Source IP Address by Region

[12] IP address that can be obtained from its host name (FQDN) or region that the IP address is allocated can change over time. In the statistics of this report, the information at the time when IPA received the information about a suspicious email and investigated it was used.

2. Distribution of the Suspicious Connecting IP address Used by Malware by Region

Figure 7 shows the regional distribution of the suspicious connecting IP address (C2 or other malicious servers) used by reported viruses. A suspicious connecting IP address means the destination IP address - likely a C2 server or other malicious server - a virus tries to establish a connection. Here, a virus means one that is embedded in attachments or downloaded onto the computer through drive-by download attacks[13] when accessing the URL written in the mail body.

According to the statistics, the 1st is the United States and accounts for nearly 30% of the total. From the 2nd to 5th are Hong Kong, China, Korea, and Japan. Those five countries account for 70% of the total. Japanese IP addresses account for 7%. When Japanese IP addresses or domain names are identified on the email delivery routes or as a suspicious connecting IP address, with authorization from the information source, we collaborated with JPCERT/CC to stop and clean the computers in question

As for the suspicious connecting IP address, just like the source IP address, an attacker may be exploiting someone else's sever or PC in order to conceal his or her identity. On the other hand, it is assumed that an attacker needs to stay in control of the computer with the suspicious connecting IP address for a certain period of time. Thus, it is guessed that there may be a different skew from Figure 6 (the source IP address) because the regions where it is easy to develop and maintain an attack infrastructure are preferred.

5% of the suspicious connecting IP addresses ended up unknown because the host names could not be resolved when the investigation was conducted[14].

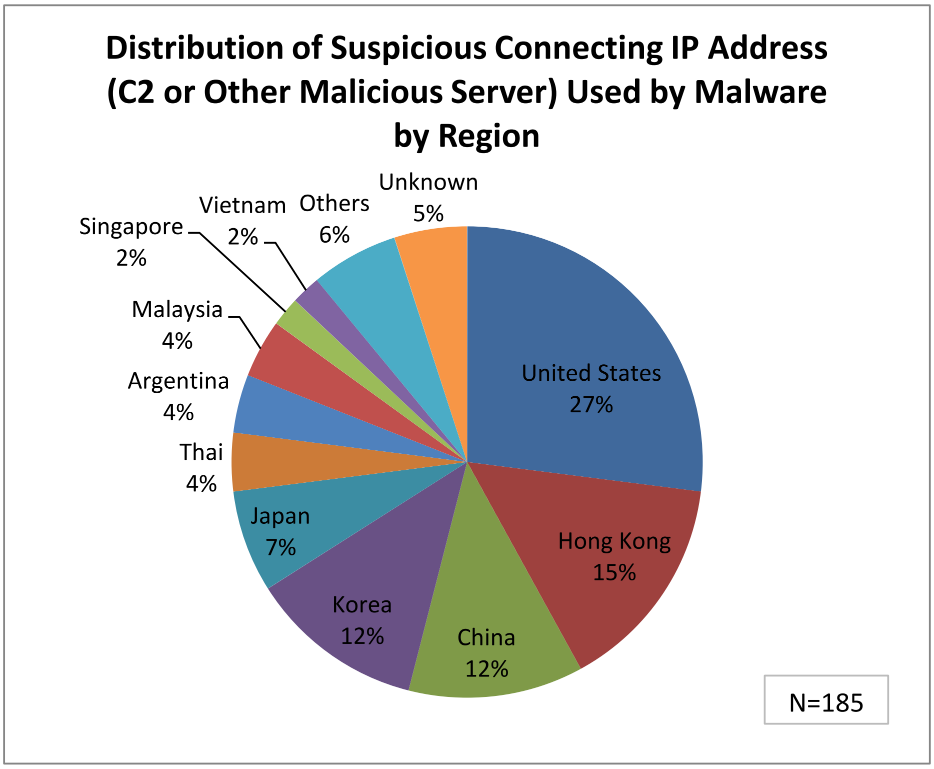

Figure 7 Distribution of Suspicious Connecting IP Addresses used by Malware by Region

[13] An attack technique that infects a PC with virus exploiting vulnerability in the PC through maliciously crafted websites. Reference: "Watch out for 'drive-by download' attack as you get infected just browsing website!" (announced in December 2010) (IPA)
http://www.ipa.go.jp/security/english/virus/press/201011/E_PR201011.html

[14] Changing a host name into an IP address when establishing a connection is called "name resolution". There are cases where an IP address cannot be obtained (name cannot be resolved) because, for example, the information has already been deleted.

3. Categorization of Attack Emails

Figure 8 shows the categorization of attack emails in terms of the attack techniques employed in each email.

The figure is categorized into three types: “attachments” where a malicious file is attached and attackers try to make the recipient open it, “URL links” where URL links are written in the mail body and a drive-by attack likely takes place when the recipient follows the links, and “information gathering” where there is no attachments nor URL links and, the sole purpose seems to be confirming the existence of the email address.

According to the statistics, “attachments” account for nearly 80% and “URL links” and “information gathering” each accounts for about 10%. In total, it is clear that sending virus as attachments is the dominating attack technique, but the recipient needs to be cautious of drive-by download attacks through URL links.

“Unknown” means unconfirmed emails, where the recipient of the suspicious emails was confirmed with log files but the emails themselves were already deleted and thus the content could not be examined.

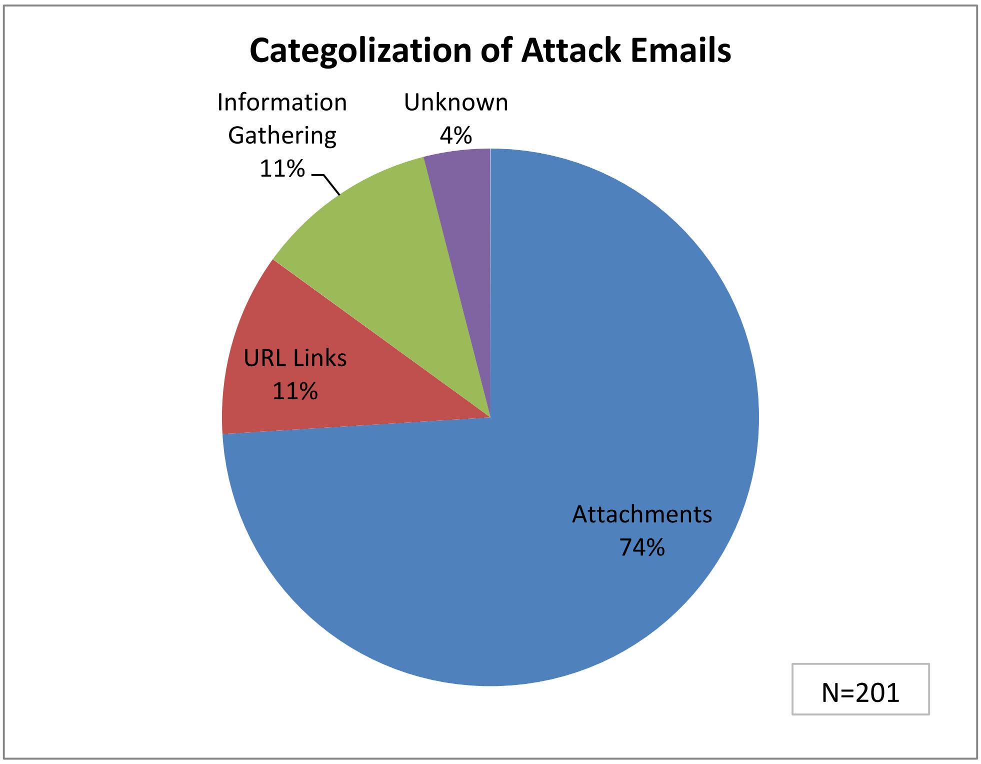

Figure 8　Type of Email/Techniques

4. Type of Attachment Files

Out of the previous section “3. Categorization of Attack Emails”, Figure 9 shows the type of malicious attachment files.

According to the statistics, “Office document files” with which virus exploits vulnerability in Microsoft Office files such as Word and Excel and “executable files” and “executable files (RLO)” with the extensions such as .exe or .scr account for more than 90% of the total.

As for the executable files, it was revealed that many are camouflaged with a document file icon to try to trick the recipient and infect with virus without bothering to exploit vulnerability. “Executable files (RLO)” are the executable files that camouflage the extension using RLO[15]. It is apparent that it is common that attackers try to make the recipient open the attachment by combining these tricks.

Also, although it is included in “Office document file” in statistics, there were small numbers of cases where vulnerabilities in Adobe Flash Player were exploited by embedding Flash objects into an Office document file.

In FY2012, the proportion of “PDF files” abuse where virus exploits vulnerability in Adobe Reader was relatively small. Additionally, small numbers of “HTML files” were identified. When the recipient double-clicks and opens the attached HTML file in web browser, it is redirected to a malicious website where a drive-by download attack is executed.

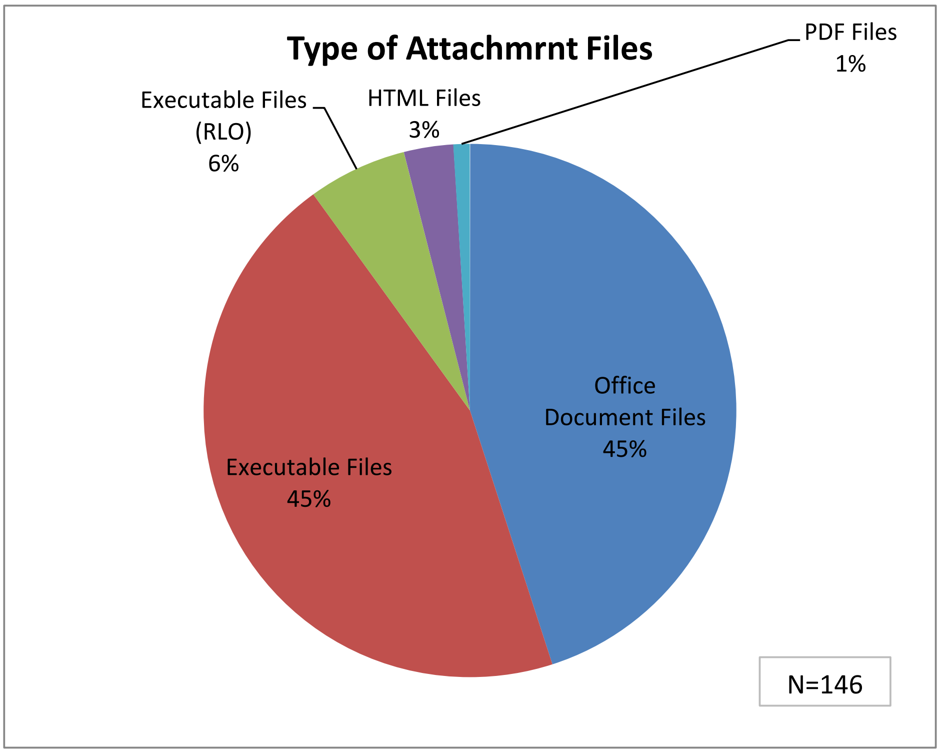

Figure 9 Type of Attachment Files

[15] ”Right-to-Left Override”. The control code that flips the order of the following characters to right- to-left.
Reference: ”Watch out for the virus that tricks you with a maliciously crafted file name” (announced in November 2011) (IPA) https://www.ipa.go.jp/security/english/virus/press/201110/E_PR201110.html

It is expected that the trends in attacks, like whether the attack method is an attachment file, drive-by download attack through URL links, or what type of attachment files is used, will change as the trends in vulnerabilities, like which ones are easy to exploit and such, change. It is necessary for the general users and the system administration departments who are responsible for raising security awareness of the employees to once again remind themselves and the employees of the following basic security measures.

- Always keep the applications up-to-date
- Make sure that an attachment file is not an executable file
- Know that the file icon or the extension can be camouflaged
- Be aware of the possibility that it can be a trap (attack) when opening an attachment file or clicking URL links written in the mail body

About the size N (the Number of Subjects) for the Graphs

The followings are the reasons that the size N (the number of subjects) for each graph is different from the “number of cases reported to IPA”.

- Among the cases reported to IPA, those that were judged as common virus emails indiscriminately and widely distributed were exempted from the statistical subjects. Thus, N is smaller than the numbers of reported cases in the “Distribution of the Source IP Address of Suspicious Emails by Region” and “Categorization of Attack Emails.”
- As for the “Type of Attachment Files”, it fluctuates up and down because there were cases where an email had more than one attachment or virus was not available since it was already removed by security tools such as anti-virus software.
- As for the “Distribution of the Suspicious Connecting IP Address Used by Malware by Region”, its N is also different from Ns in other graphs because there were cases where more than one virus is generated from an attachment or a virus tries to establish a connection with more than one IP address.