JPCERT CC®

Research Report on IT Security Inoculation

FY2009

JPCERT Coordination Center

January 21,2011

Contents

Table of Contents of Figures

1 Introduction

1.1 Targeted Email Attacks and its Background

It has been said long since that the nature of threats on the Internet has changed from fun-seeking or demonstration of technical abilities, to pursuing financial return. It can be said that the change is from self-revealing and broadly diffused threats to secret and targeted threats.

Trying to exploit cashable information (including credit card numbers, online bank account numbers, and confidential information relating to national defense, public safety, and industries) from targeted small groups is called "Targeted Attacks" in foreign countries. There are several types of targeted attacks of which one is spear phishing. This type of attack targets a specific group. Targeted email attacks, described later, belong to this type of attack.

The typical tactic of a targeted email attack is as follows: an attack email is sent to a targeted small group of recipients. The mail subjects and content of attack emails attract the recipients' attention by indicating relevant topics such as internal business communications, latest news topics, questionnaires, and attempt to induce them into opening an attached file or clicking on a URL. As a result, malware, such as Trojan horse programs may be activated, or the recipient may be directed to a website that is embedded with such software. Once the computer is infected by a malware, attacking activities tend to proceed to attempts in taking over control of the computer by embedding key-loggers.

Recently, more malicious tactics have been recognized where emails exchanged between companies or within an organization are stolen and then attack emails based on those are created to launch very sophisticated attacks.

Damages of targeted email attacks are not publicized much but are considered large. For actual details of such damages, refer to the report by the JPCERT Coordination Center (JPCERT/CC), "Research of Targeted Attacks" (in

Japanese only), which is about a research conducted based on questionnaires to companies in Japan.

1.2 Objectives of this Research

Under these circumstances, JPCERT/CC has investigated actual situations of targeted attacks and evaluated inoculation methods, and the outcomes were reported for each fiscal year as “Research of Targeted Attacks” for 2006, “Research Report on Measures to Deal with Targeted Attacks[1]” for 2007, and “Research Report on IT Security Inoculation[2]” for 2008. While details of the research are given in the reports, the research has revealed that targeted email attacks do indeed exist and that education and training based on inoculation methods proved effective to a certain level.

This year (2009), the third fiscal year for such research, we perform the same investigation with the following three objectives in the Research of IT security inoculation (also referred to as “Inoculation” or “Inoculation 2009” for short).

1. Confirm how inoculation methods are effective in acquiring tolerance against targeted email attacks.
2. Investigate the maintained level of learning effect over time in organizations that have experienced inoculation in fiscal year of 2008.
3. Attempt to verify the new hypothesis of risk groups (“People who deal with large amounts of email within a short time are exposed to higher risks”, “Pseudo attack emails with mail subjects or content related to one’s own business pose a higher risk”).

---

1 http://www.jpcert.or.jp/research/#targeted2
2 http://www.jpcert.or.jp/research/#inoculation

2 Method of Investigation

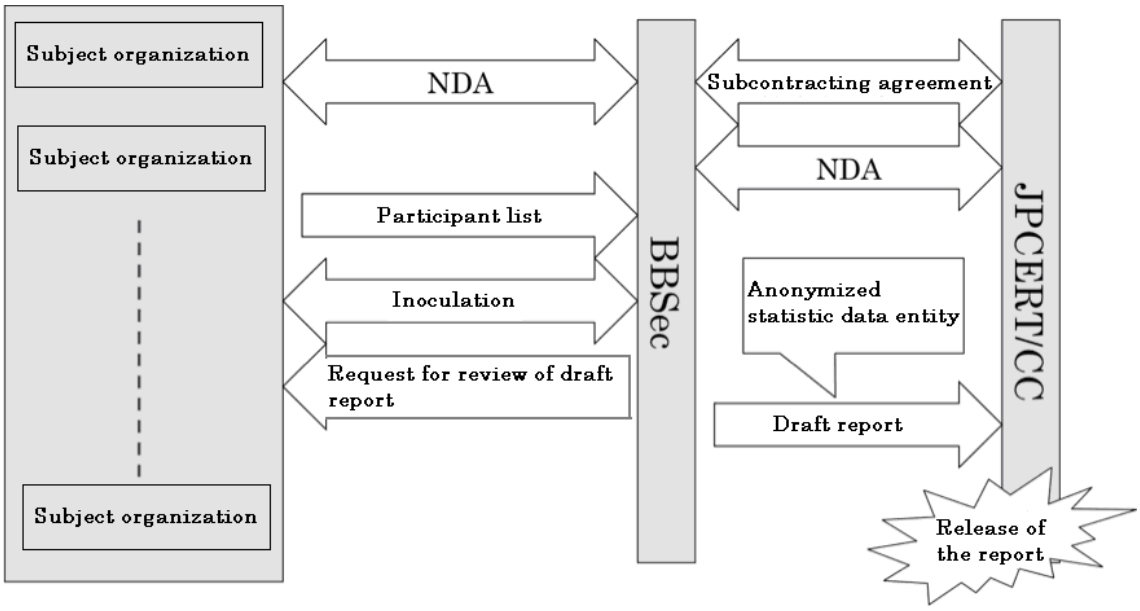
2.1 Investigation System and Security Protection

The Inoculation Research of fiscal year 2009 was subcontracted to Broad Band Security, Inc. (BBSec). In addition to a subcontracting agreement, a nondisclosure agreement (NDA) was concluded between JPCERT/CC and BBSec in order ensure nondisclosure of the subject organization's confidential information. An NDA was also made between each subject organization and BBSec. This was done to allow subject organizations to provide email addresses within the list of participants from the organization which is required for the research of inoculation.

Information of names of all subject organizations are shared between JPCERT/CC and BBSec, but in publicized information related to this report, only those information permitted by the organizations are disclosed.

In addition, this report has been reviewed by each organization before its release in order to make sure that no descriptions are in violation of the NDA.

Fig. 2-1) Investigation Framework and Confidentiality



2.2 Overall Investigation Flow

Investigation was performed according to the following flow. Here we only focus on the overall investigation flow. Details will be explained later.

(1) Conclusion of NDA with subject organization

NDAs were concluded before commencement of investigation in order to establish a basis for maintaining confidentiality in subsequent tasks.

(2) Selection of date to perform inoculation

Two candidate dates were suggested for the subject organization to choose from.

(3) Selection of pseudo attack email type and arrangement of email attachment file content

Six different types of pseudo-attack email were presented from which two were selected by the subject organization. In addition, the organization checked and edited as necessary, the message that would be shown when the attachment file of a pseudo-attack email is opened.

(4) Prior-education at subject organization

Subject organizations held education sessions for their end-users two to four weeks before the pseudo-attack emails were to be delivered.
The education included topics such as what targeted attack emails are, that they are spreading, and that they should be aware of them.

(5) Preliminary exercises and system preparation

As preliminary exercise, pseudo-attack emails, which are much like those sent as actual ones, were sent only to persons in charge in each subject organization. This was aimed for persons in charge to understand how actual pseudo attacks would look like and to confirm there are no issues there. Furthermore, there may be cases where they are asked to

temporarily alter their anti-spam settings such as firewall configurations.

Also, access to the website of questionnaires for subject organizations was confirmed.

(6) Submission of list of subject participants

Participants from each organization were selected and a list of their email addresses was submitted to us.

(7) Delivery of pseudo-attack emails

Pseudo-attack emails were sent two times with a two weeks interval. When an attachment of the pseudo-attack email is opened, a web beacon is activated and a record is written into the log on the Web server at BBSec.

(8) Explanation of the research by the subject organization

Each time pseudo attack email is sent, the person in charge waited for a certain interval until all users have read the email, and then explained about the research.

(9) Questionnaire

After the two deliveries of the pseudo attack emails, subject participants were asked to fill out a questionnaire. The questionnaire for the participants was a web-based questionnaire.

(10) Informing the total count of web beacon records in the log

After revealing the research experiment on each delivery, web beacon records in the logs were counted up and informed to each of the subject organizations.

(11) Informing the result of the questionnaire

Results of the questionnaire were summarized and informed to each of the subject organizations.

(12) Review of draft report by each subject organization

Before the release of the research report on IT security inoculation for the 2009 fiscal year, a draft of the report was reviewed by each subject organization.

(13) Release of the report

The results of this research are summarized in this report.

2.3 Schedule

For the research this year, subject organizations were asked to select, in principle, either one of the two schedule dates shown below. Also, there had been a subject organization that performed a test-inoculation before these listed schedule dates.

Fig. 2-2) Candidate Schedule Dates by Group

Group a	Group b	Details
Sep 1, 2009		Notification to subject organizations that have participated in the 2008 fiscal year
Sep 10		Application deadline
Sep 1 to Sep 30	Sep 1 to Oct 16	NDA conclusion System preparation (e.g. spam filters) Submission of participant list
Oct 1	Oct 20	Delivery of pre-education email
Oct 14	Nov 4	First pseudo-attack email delivery Delivery of explanation email
Oct 28	Nov 18	Second pseudo-attack email delivery Delivery of explanation email and request for responding to questionnaire
Oct 29/Nov 6	Nov 18/Nov 25	Answers to questionnaire collected
Nov 4	Nov 24	Quick results report (web beacon count up)
Nov 11	Nov 30	Quick results report (summary of answers

		to questionnaire to participants was tabulated)

2.4 Participant List

Participant lists with email addresses (required) and names (optional) of participants were obtained from each organization. Needless to say, personal information in these participant lists were used only for delivering pseudo-attack emails.

Only personal mail addresses of the participants were used. Aliases and mailing list addresses which distribute mail to multiple recipients were avoided. This is because when attack emails are sent to such email addresses, it is not possible to tell how many recipients have opened the attachment just from the web beacon log.

Fig. 2-3) Participant List

Subject Organization #.	#	Name	Email address	Remarks
1000	0	Yobou Sessyu	yobou@example.jp	Example
	1			Please fill out the fields surrounded by the double line
	2			
	3			
	:			

2.5 System Related Preparations

For the inoculation research of the 2009 fiscal year, some subject organizations will need to alter their IT security measures in order to deliver pseudo-attack emails and filling out the questionnaire for participants.

First, since pseudo attack emails are sent from a certain server of BBSec, organizations were asked to include this server in their spam filter's white-list.

Also, since this same server is used to establish Web servers for logging the web beacons and supporting the questionnaire, the organizations were asked to allow HTTP (80/tcp) and HTTPS (443/tcp) access to this server. When collecting logs or proving the questionnaire, random meaningless characters that are difficult to guess are used in the URL in place of the subject organization's name because if the name is used as-is, the organization's name may become exposed.

2.6 Pre-Education Material

In this research, a template for pre-education material was prepared and provided to subject organizations. They did not necessarily have to use this template but our expectations were that they could save their time by using this template as draft.

Note that descriptions in this report may be based on an assumption that pre-education is done via email. However, the intention is to have pre-education done in the organization's normal way, and does not necessarily have to be distributed via email. It is desirable for the pre-education material to be distributed via email two to four weeks before the actual pseudo-attack emails are delivered.

The point is in preventing the participants from feeling offended which may reduce the effectiveness of inoculation when it is performed without

pre-education and prior announcement. It is worth reiterating that there had been several cases of unannounced inoculations of which none were able to yield good results.

Fig. 2-4 shows the template for pre-education material.

Fig. 2-4) Template for Pre-Education Material

August 5, 2009

X Company Research Development Section

Person in charge: Yobou Sessyu

(03)CDEF-xxxx

Targeted email attacks

Thank you for your on-going cooperation concerning our IT security measures. Recently, "targeted email attacks" is emerging as a threat, and as such, we hereby promote awareness as follows:

Three points to remember

A) Targeted email attacks are still silently widespread, and you are also at risk.

B) Targeted email attacks try to take control of your PC by inducing you to open an attachment file.

C) In order to prevent targeted email attacks from succeeding, recipients of such email mus be able to identify a suspicious email. In the event you receive a suspicious email, please inform the person in charge of security at or around your department.

(1) Background of targeted email attacks

It has been said the objective of hackers on the Internet has changed from "fun-seeking or demonstration of technical abilities" to "pursuing financial return", and the tactics has been changed from "self-revealing and widespread" to "secret and targeted".

Especially, targeted email attacks are a typical example of the new threat which "target small groups", and "try to exploit cashable information". Exploited cashable information would generally include credit card numbers, online bank account passwords, and confidential information relating to national defense, public safety, and industries, etc...

(2) Tactics of targeted email attacks

Targeted email attacks start by sending attack emails to a targeted small group of recipients. The attack emails attract the recipients' attention by indicating relevant topics (such as pretending to be a mail on latest news or internal business communication), and persuades the recipient to open attachment files.

Once the recipient opens an attachment file, malware embedded in the attachment file (malicious program) activates and performs malicious acts such as stealing various information from the PC. Recent malware operate in "stealth" mode to avoid being noticed while carrying out malicious acts. So, there may be cases where a key-logger is installed silently and key input is constantly monitored.

1

(3) Examples of targeted email attacks

Unfortunately, examples of targeted email attacks are seldom published. Presumably, this is because the recipient has not noticed the attacks, or they refrain from publicizing the incident considering the effect on their reputation.

Case studies and researches available to the public are:

In the JPCERT/CC Questionnaire survey (2007), the questionnaire was answered anonymously via postal mail by a total of 282 companies of which 6.4% answered that they experienced a targeted attack within the last 12 months.[i]

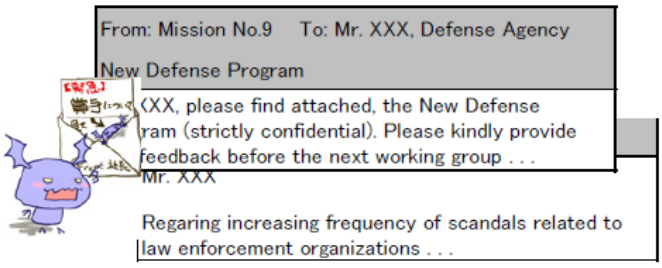
Are attacks increasing?

The survey asked whether organizations have experienced targeted attacks and whether the attack had occurred within the past year (from April 2006 to March 2007). The results are shown in the table below:

Method of attack	Number of organizations that experienced	Percentage within total number of organizations
Spear Phishing	7 (7)	2.6% (2.5%)
Virus attached emal sent to personnel from someone imposing as a related person	18 (15)	6.5% (5.4%)
Blackmail threating to perform a DoS attack	3 (2)	1.2% (0.8%)

Numbers in parentheses are occurrence in past year

From the JPCERT/CC Questionnaire Survey (2007) Report



Sample image of the targeted

Furthermore, the National Police Agency lecture at the Shirahama Symposium (2006) mentioned experiences of targeted email attacks where the National Police Agency received a mail titled "Handling of Misconduct", and the Defense Agency received a mail titled "Next National Defense Plans".[ii]

There were other cases of attacks such as receiving emails with titles like "Prime Minister Koizumi visited Yasukuni Shrine", "About Taiwan situation", or receiving an email with an attachment that is named "Event Plan 2007.lzh".[iii]

(4) Countermeasures against targeted email attacks

As countermeasures against targeted mail attacks, it is very important to steadily implement technical measures such as anti-spam measures or information leakage prevention measures. However, due to the nature of targeted email attacks which "target small groups" of recipients, you would have to say that it is difficult to prevent damage completely by performing technical measures alone.

That is why it has become important for "individual email recipients to spot suspicious emails". Emails that match the characteristics listed below are likely to be targeted email attacks, although there may be variations depending on capability of the attacker or other situations. (Of course, there are possibilities that an email is a normal email instead of a targeted mail attack. This makes

implementation of countermeasure difficult.)

Characteristics of a suspicious email

- Name or address of the sender is unfamiliar
- Mail has been sent from external mail address, although the topics are internal to the organization.
- The email tries to unnaturally induce recipients into opening an attachment file.
- The e-mail pressures the recipient using the phrase such as "urgent" and tries not to let you carefully contemplate its content
- The sender's name and/or signature are missing or are ambiguous.
- They sender's name and/or organization name is fake.

Be sure to pay closer attention such as examining sender's information (name or email address, etc.) when processing emails. If you find suspicious emails, do not open them directly. And take measures such as asking with the sender of the email, or contacting the security personnel near you, etc.

---

[i] http://www.jpcert.or.jp/research/2007/targeted_attack.pdf

[ii] http://itpro.nikkeibp.co.jp/article/NEWS/20060529/239209/

[iii] http://www.itmedia.co.jp/enterprise/articles/0510/20/news118.html
http://itpro.nikkeibp.co.jp/article/COLUMN/20070307/264174
http://biz.plala.or.jp/support/security/backnum/2007/070628.html

3

2.7 Pseudo-Attack Email

In this research, pseudo-attack emails (templates with subject and body text) were prepared from which subject organizations were to choose the email to use. The intention was to make it possible to compare the attachment opening ratio between subject organizations and “strength” between pseudo-attack email types.

Note that the name portion of the sender could be modified to a “realistic but non-existing” name if required. Furthermore, the domain name used for the sender was registered specially for the inoculation.

Details of the six different pseudo-attack emails are shown below in **Fig.2-5** to **Fig.2-10**.

Fig.2-5) Pseudo-Attack Email S: Influenza

Subject	Emergency! New influenza may become highly-virulent
From	Committee of Influenza Measures <oshirase@SwineFluInfo.jp>
Body	The new strain of influenza viruses has been reported to be highly contagious but with rather low virulence. However, a highly-virulent new strain of influenza virus has appeared, and infected individuals are rapidly increasing. Please refer to the attached “Influenza measures to be taken immediately” and reinforce your measures. Initial response is very important in countering the new influenza. Act now to prevent a pandemic from spreading out from Japan. Committee of Influenza Measures
Attachment Name	Influenza measures to be taken immediately.doc

Customization	Change the name “Committee of Influenza Measures” to a different name that looks realistic but does not actually exist in each subject organization.
Points that should be recognized	1. The sender’s display name contains a non-existing organization name. 2. The sender's email address domain is external. 3. The sender's email address is not familiar. 4. The mail attempts to induce the recipient to open the attachment file. 5. The mail pressures the recipient by mentioning the word “pandemic”. 6. The signature does not contain address and contact information.

Fig.2-6) Pseudo-Attack Email T: Business Continuity Plan

Subject	Reconsideration of business continuity plan for major earthquakes
From	Business Continuity Plan Committee <drc@jigyokeizoku.jp>
Body	The Tomei Expressway five-day-shut down due to the landslide of the slope in Makinohara area, which was caused by the earthquake that hit the Tokai area on Aug. 11, 2009, is still a fresh memory. The seismic center was off the Suruga Bay. Learning lessons from this disaster, we have decided to conduct a special review of our business continuity plan. We would appreciate your cooperation for the current situation survey by following the instructions in the attached file. All employees are required to replete since the items surveyed include commuter routes (including the return-home route at the time of disaster) of each

	employee. We appreciate your cooperation. Business Continuity Plan Committee
Attachment Name	Business continuity plan current situation check sheet 3.doc
Customization	Change the name “Business Continuity Plan Committee” to a different name that looks realistic but does not actually exist in each subject organization.
Points that should be recognized	1. The sender’s display name contains a non-existing organization name. 2. The sender's email address domain is external. 3. The sender's email address is not familiar. 4. The mail attempts to induce the recipient to open the attachment file. 5. The mail pressures the recipient by mentioning disaster and business continuity plan. 6. The signature does not contain address and contact information. 7. There is a typo. ("replete" should be replaced by "reply")

Fig.2-7) Pseudo-Attack Email U: Intranet System

Subject	Urgent questionnaire
From	Information System Department <syuukei@mail1ban.jp>
Body	We would appreciate you to fill out a questionnaire regarding the usability of the intranet system. Please do not hesitate to express your frank opinions. The intranet system has many subsystems including Web interface systems. However, we hear that all of them have poor usability.

	Thus, in an aim to improve work efficiency etc., we are collecting opinions from a broad base Please kindly fill out the attached questionnaire and replete as soon as possible. Information System Department
Attachment Name	Questionnaire template.doc
Customization	Change the name “Information System Department” to a different name that looks realistic but does not actually exist in each subject organization.
Points that should be recognized	1. The sender's email address is not familiar. 2. The sender's email address domain is external. 3. The mail attempts to induce the recipient to open attached questionnaire. 4. The mail pressures the recipient by saying “Reply as soon as possible”. 5. The signature is missing.

Fig.2-8) Pseudo-Attack Email V: Information Leakage Incident

Subject	Announcement regarding an information leakage incident
From	Committee of Personal Information Protection Measures <kakunin@kojoho.jp>
Body	The Committee of Personal Information Protection Measures has been informed of the possibility that information regarding your credit card may have leaked. In response, we are now checking the internal status of the company. Both those who think they are relevant and those who do not should check. Therefore, please kindly fill out necessary information in the attached document and send it back to

	us. Should your credit card number be abused, financial damage may result. Your urgent action is necessary.
Attachment Name	038-Credit card query.doc
Customization	Change the name “Committee of Personal Information Protection Measures” to a different name that looks realistic but does not actually exists in each subject organization.
Points that should be recognized	1. The sender’s display name contains a non-existing organization name. 2. The sender's email address domain is external. 3. The mail attempts to induce the recipient to open the attachment file by mentioning the possibility of damage. 4. The mail pressures the recipient by saying “Reply as soon as possible”. 5. The signature is missing.

Fig.2-9) Pseudo-Attack Email W: Windows Patch

Subject	Urgent: Temporary workaround for Windows vulnerability
From	Information System Department Emergency Response Team <info@joshisu.jp>
Body	A serious Windows vulnerability was found yesterday. Currently, there is no patch available. However; a temporary workaround is provided. Follow the attached instructions to apply the workaround as soon as possible. The vulnerability allows your PC to be taken over control remotely, so your immediate action is necessary. Information System Department Emergency Response Team
Attachment Name	Temporary workaround instructions.doc

Customization	Change the name “Information System Department Emergency Response Team” to a different name that looks realistic but does not actually exist in each subject organization.
Points that should be recognized	1. The sender’s display name contains a non-existing organization. 2. The sender's email address domain is external. 3. The mail attempts to induce the recipient to open the attachment by referring to it as an instruction document. 4. The mail pressures the recipient by urging to take action immediately. 5. The signature does not contain address and contact information.

Fig.2-10) Pseudo-Attack Email X: JS Alert

Subject	Urgent: Alert regarding JavaScript etc.
From	Information System Department Emergency Response Team <security@joshisu.jp>
Body	To whom it may concern, Recently, there is an increasing number intrusion attempts that exploit JavaScript security holes of a browser (e.g. Internet Explorer). The same kinds of problems are found with other browsers as well as script languages similar to JavaScript. Not all, but most risks can be mitigated by applying appropriate settings. Therefore, follow the instructions in the attachment to check your browser settings as soon as possible, and apply safer setting.

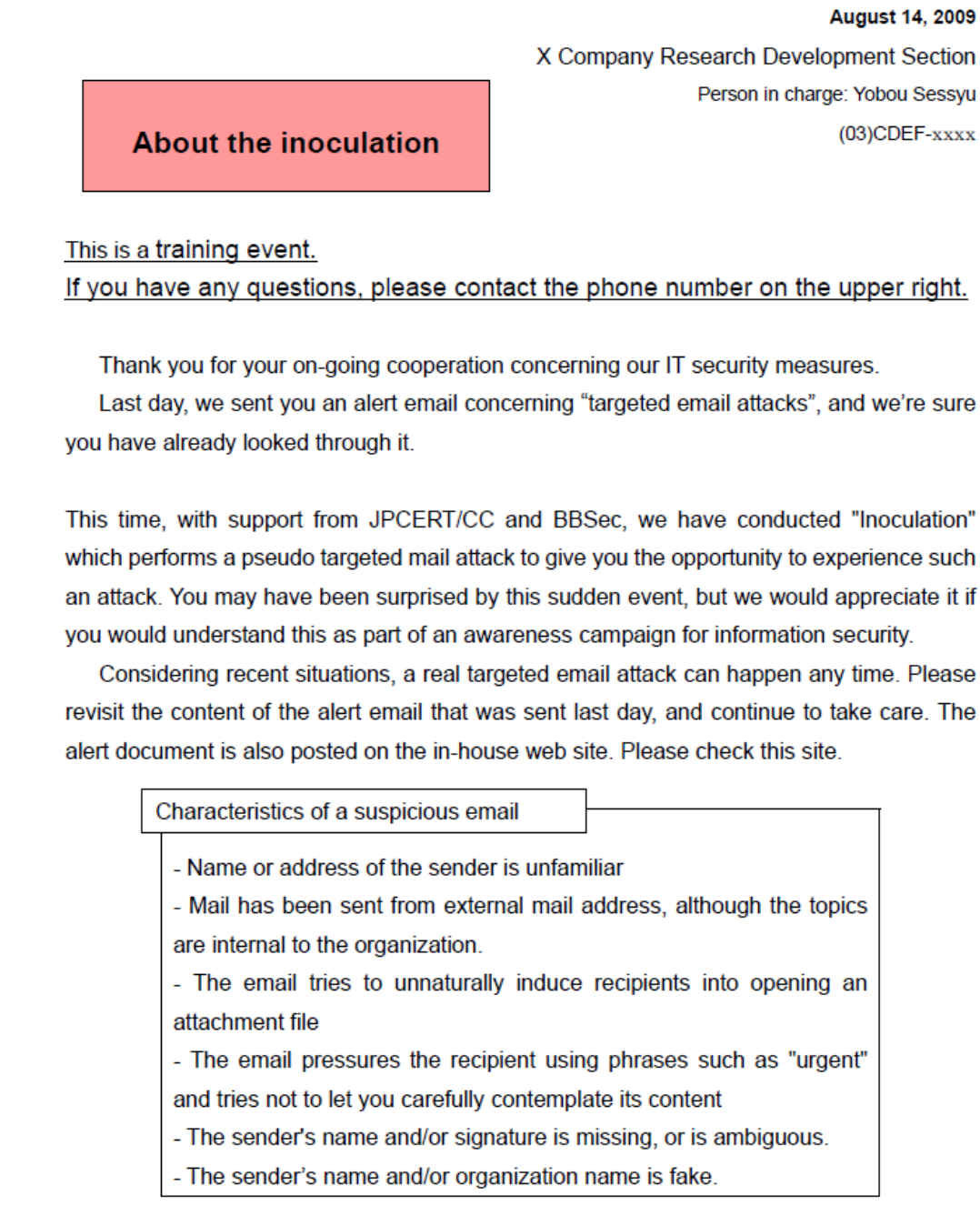
	Information System Department Emergency Response Team
Attachment Name	Checking instruction.doc
Customization	Change the name “Information System Department Emergency Response Team” to a different name that looks realistic but does not actually exist in each subject organization.
Points that should be recognized	1. The sender’s display name contains a non-existing organization. 2. The sender's email address domain is external. 3. The mail attempts to induce the recipient to open the attachment by referring to it as checking instructions. 4. The mail pressures the recipient by urging to take action “as soon as possible”. 5. The signature does not contain address and contact information.

2.8 Attachment of Pseudo-Attack Email

Pseudo attack emails were attached with a Microsoft Word format file embedded with a Web beacon function. When a recipient opens the attachment as a result of being induced by subject line and body content of the pseudo-attack email, the Web beacon is triggered and recorded in the log collection server to be counted as a recipient who opened the attachment.

Contents of the attachment file are shown in **Fig. 2-11**. However; at least the contact information including organization name, department, and name of a person in charge should be changed in accordance with each organization. Other information may also be changed in accordance with the actual situations of each organization.

Fig. 2-11) Attachment for Pseudo-Attack Emails



August 14, 2009

X Company Research Development Section

Person in charge: Yobou Sessyu

(03)CDEF-xxxx

About the inoculation

This is a training event.
If you have any questions, please contact the phone number on the upper right.

Thank you for your on-going cooperation concerning our IT security measures.
Last day, we sent you an alert email concerning “targeted email attacks”, and we’re sure you have already looked through it.

This time, with support from JPCERT/CC and BBSec, we have conducted "Inoculation" which performs a pseudo targeted mail attack to give you the opportunity to experience such an attack. You may have been surprised by this sudden event, but we would appreciate it if you would understand this as part of an awareness campaign for information security.

Considering recent situations, a real targeted email attack can happen any time. Please revisit the content of the alert email that was sent last day, and continue to take care. The alert document is also posted on the in-house web site. Please check this site.

Characteristics of a suspicious email

- Name or address of the sender is unfamiliar
- Mail has been sent from external mail address, although the topics are internal to the organization.
- The email tries to unnaturally induce recipients into opening an attachment file
- The email pressures the recipient using phrases such as "urgent" and tries not to let you carefully contemplate its content
- The sender's name and/or signature is missing, or is ambiguous.
- The sender’s name and/or organization name is fake.

2.9 Revealing the Research

Each time after pseudo-attack emails were sent, the research was revealed by the person in charge at each subject organization to eliminate any uncertainties of the participants. The persons in charge were asked to keep the following in

mind when revealing the research.

(1) Emphasize the following:

  (a) The delivered pseudo-attack emails are just exercises and do not cause actual damage.
  (b) Individuals are not evaluated by the results of this research

(2) Revealing should take place on the evening of the day the pseudo-attack emails were delivered.

(3) On the second round of revealing, ask the participants to fill out the questionnaires.

Template explanations shown in **Fig. 2-12** and **Fig. 2-13** were prepared and distributed to subject organizations to use and modify as necessary.

Fig. 2-12) Draft Template of Explanation (1st time)

To all employees,

Committee of Information Security Measures
Person in charge: Yobou Sessyu

About the Inoculation Test (report)

Thank you for your on-going cooperation with our IT security measures.

Today, an “inoculation” was conducted for education and training purposes to prepare you against targeted email attacks.
The inoculation involves performing a pseudo targeted email attack to allow you to experience the attack and to be prepared for actual attacks. Even if you have not handled the training sufficiently, no actual damage is caused, and no negative evaluations will be recorded. We hope you will utilize the outcome of this training to be prepared.

In an awareness raising promotion performed on <Month> <Date>, we have provided information such as, what targeted email attacks are, and how to handle such attacks. An explanation document is posted on our internal company website, so please revisit and check the document. The file name of the document is “About targeted email attacks.doc”.

The “Three Points to Remember” are as follows:

A) Targeted email attacks are still silently widespread, and you are also at risk.

B) Targeted email attacks try to take control of your PC by inducing you to open an attachment file.

C) In order to prevent targeted email attacks from succeeding, recipients of such email must be able to identify a suspicious email. In the event you receive a suspicious email, please inform the person in charge of security at or around your department.

You should continue anticipating targeted email attacks. Therefore, be aware of the following “characteristics of suspicious email” and handle with care.

- Name or address of the sender is unfamiliar.
- The email was sent from an external email address, although the topic is internal to the organization.
- The email induces you unnaturally to open the attachment.
- The email pressures you for quick action by using words such as “urgent”, and tries not to let you contemplate carefully.
- The sender's name and/or signature is missing, or is ambiguous.
- The sender’s name and/or organization name are fake.

Fig. 2-13) Draft Template of Explanation (2nd time)

To all employees,

Committee of Information Security Measures
Person in charge: Yobou Sessyu

About the Inoculation Test (report)

Thank you for your on-going cooperation with our IT security measures.

Today, a follow-up “inoculation” was conducted for education and training purposes to prepare you against targeted email attacks.
The inoculation involves performing a pseudo targeted email attack to allow you to experience the attack and to be prepared for actual attacks. Even if you have not handled the training sufficiently, no actual damage is caused, and no negative evaluations will be recorded. It is sufficient that you utilize the outcome of this training to be prepared.

In an awareness raising promotion performed on <Month> <Date>, we have provided information such as, what targeted email attacks are, and how to handle such attacks. An explanation document is posted on our internal company website, so please revisit and check the document. The file name of the document is “About targeted email attacks.doc”.

For your information, this inoculation was performed by BBSec as a research project for JPCERT/CC. The results will eventually be published as a report. Rest assured that names of subject organizations as well as names and addresses of individual participants will not be disclosed unless permission has been granted.

JPCERT/CC and BBSec are requesting for cooperation with a questionnaire in order “learn from your experience of the inoculation in order to prepare countermeasures against targeted email attacks”. Please kindly cooperate in

filling out this anonymous questionnaire wherever possible. (Cookies are used to prevent the same person filling out the questionnaire more than once. The cookies do not contain information that can be used to identify an individual.)

The questionnaire is posted on the following URL:
https://inoculation2009.randd.bbsec.co.jp/<unique hash number for subject organization>
(Questionnaires are accepted from <Month> <Date> to <Month> <Date> .)

2.10 Questionnaire

In this research, participants' attribute information and email opening status were collected through a questionnaire.
Considering the effort of summarizing the responses, the questionnaire was posted on a website, and to make the respondents feel more at ease, the questionnaire was made to be answered anonymously.
The questions of the questionnaire are listed in **Fig. 2-14**.

Fig. 2-14) Questions in the Questionnaire

IT Security Inoculation 2009 Questionnaire

Thank you for your cooperation on the IT security inoculation 2009.

The IT Security Inoculation is conducted as a research project of JPCERT coordination center (JPCERT/CC) and is conducted by Broad Band Security (BBSec).
We appreciate your further cooperation to fill out this questionnaire.

The results of the research will be documented as a report which will be published.
Answers to the questionnaire will also be used in the report.
Your personal information and organization name will be handled as

anonymous, and as such, will not be disclosed. (In some cases, organization names will be disclosed after permission is granted.))
Cookies (15-digit random alpha-numeral characters, expires in 90 days) are used to prevent the same person from submitting multiple instances of the questionnaire.
The report from the previous fiscal year is published by JPCERT/. Please refer to that report to find out how anonymous information is used.
Thank you for your cooperation.

Please contact the department in charge for the inoculation or BBSec Inoculation Team (<email address>).

IT Security Inoculation 2009 Questionnaire

Q1) Choose your gender.

1. Male
2. Female

Q2) What is your age group.

1. Below 20
2. 20 to 29
3. 30 to 39
4. 40 to 49
5. 50 to 59
6. Above 60

Q3) What is your duty? Choose the one closest.

1. Executive officer
2. Manager
3. Sales/Marketing
4. Service/Customer support
5. Clerical work
6. Computer engineer

7. Other engineer

Q4) How much are you skilled in business email communication?

Choose one most applicable

1. Highly skillful
2. Skillful
3. Average
4. Unskillful
5. Poor

Q5) How many business emails do you send and receive every day?

Average of _____ emails per day (weekdays)

Q6) How long does it take to handle one business email?

Answer in total hours of your time to deal with each email. Round up minutes to the nearest hour.

Average of _____ hours in total per day (weekdays)

Q7) Have you experienced IT security inoculation in the past?

Last fiscal year's inoculation took place between August 2008 and March 2009 using the same method as this year.

1. Experienced (as participant)
2. Not experienced (first time this year)

Q8) How did you respond to this year's 1st delivery of pseudo-attack email?

This year's first pseudo-attack email was delivered on November 4th with the subject, "Information leakage Incident".

1. I received the email and opened the attachment file.
2. I received the email but did not open the attachment file.
3. I did not receive such email.

Q9) How much were the subject and email content related to your work?

Choose one most applicable.

1. Very much related
2. Much related
3. Slightly related
4. Not related

Q10) How did you respond to this year's 2nd delivery of pseudo-attack email?

The second pseudo-attack email was delivered on November 18th with the subject, "Emergency! New influenza may become highly-virulent".

1. I received the email and opened the attachment file.
2. I received the email and but did not open the attachment file.
3. I did not receive such email.

Q11) How much were the subject and email content related to your work?

Choose one most applicable.

1. Very much related
2. Much related
3. Slightly related
4. Not related

Q12) Write freely any comment or opinion on the inoculation (Up to 400 letters. You can also leave this blank.)

Send (I confirmed the content)

If you are returned to this page after pressing the button above, the questions in red (mandatory questions) need to be answered. Answer the question(s) as appropriate.

If you answer the questions appropriately, the answers are sent and the

questionnaire finishes. Thank you for your cooperation.

2.11 Recruitment and Selection of Subject Organizations

For this research, we mainly asked for cooperation of organizations that have experienced the inoculation in the fiscal year of 2008. This is because one of our aims was to investigate improvement over time.

Fig 2-15 lists the selected subject organization this year.

Fig 2-15) Subject Organization and Number of Individual Participants

Subject Organization	Business Field	Schedule	Number of Participants
A	Security measures service BroadBand Security, Inc.	b	63
B	Transport	b	161
C	Communication service	b	1,154
D	Critical infrastructure system integrator	b	198
E	R&D in energy business	b	881
F	Web service	a	282
G	Mechanical industry	b	188
H	Study, advise, and coordination of security related measures (Japan Computer Emergency Response Team Coordination Center)	Preceding	31
(Total)			2,958

Conditions on pseudo-attack email delivery and subject's questionnaire varies depending on the subject organization. Those differences are listed below.

1. Subject organization F delivered 2nd pseudo-attack emails on Oct. 30, 2009 due to business matters. This date was 2 days behind the schedule for

group “a”. Questionnaires were also delayed accordingly. This schedule change is considered to not affect much to the result of the inoculation.

2. Subject organization G installed the server for collecting web beacon logs within the premises of G. This is considered not to affect much to the result of the inoculation.

3. Subject organization G used their own system to obtain answers to the questionnaire. Because of this, part of the answers to the questions could not be summarized or analyzed as their relations were unknown.

4. Subject organization H provided mailing list addresses for part of the list of participants. Therefore, these data could not be used in the summarization or analysis of web beacon logs as well as the questionnaire

5. Subject organization H performed inoculation before other organizations. The inoculation of organization H is considered as a preliminary investigation to check work procedures, and therefore not used in the summarization and analysis of the questionnaire.

6. Subject organizations, A, B, C, D, E, G and H participated in the research of both fiscal years of 2008 and this year. Subject organization F participated in the inoculation for the first time this fiscal year.

3 Results of Inoculation as seen from Web Beacon Log

3.1 Results per Subject Organization

Fig. 3-1 shows the Number of Participants per Subject Organization, the Pseudo-Attack Email Used, the Number of Participants (each time) who opened the attachment of a Pseudo-Attack Email at the time of delivery, and the Ratio of the Total Number of Participants who opened the Email attachment to the Total Number of Participants (ratio of email opening). Furthermore, the Improvement Rate is calculated by deducting “the Ratio of Attachment Opening at 2nd Delivery” from “the Ratio of Attachment Opening at 1st Delivery”.

(Improvement Rate) = (Ratio of Attachment Opening at 1st Delivery) – (Ratio of Attachment Opening at 2nd Delivery)

A High Improvement Rate means that the Ratio of Attachment Opening has dropped (improved) significantly at 2nd delivery compared to 1st delivery. This value had also been used as an evaluation index in the Inoculation Survey of fiscal year 2008.

Fig. 3-1) Web Beacon Data and Improvement Rate

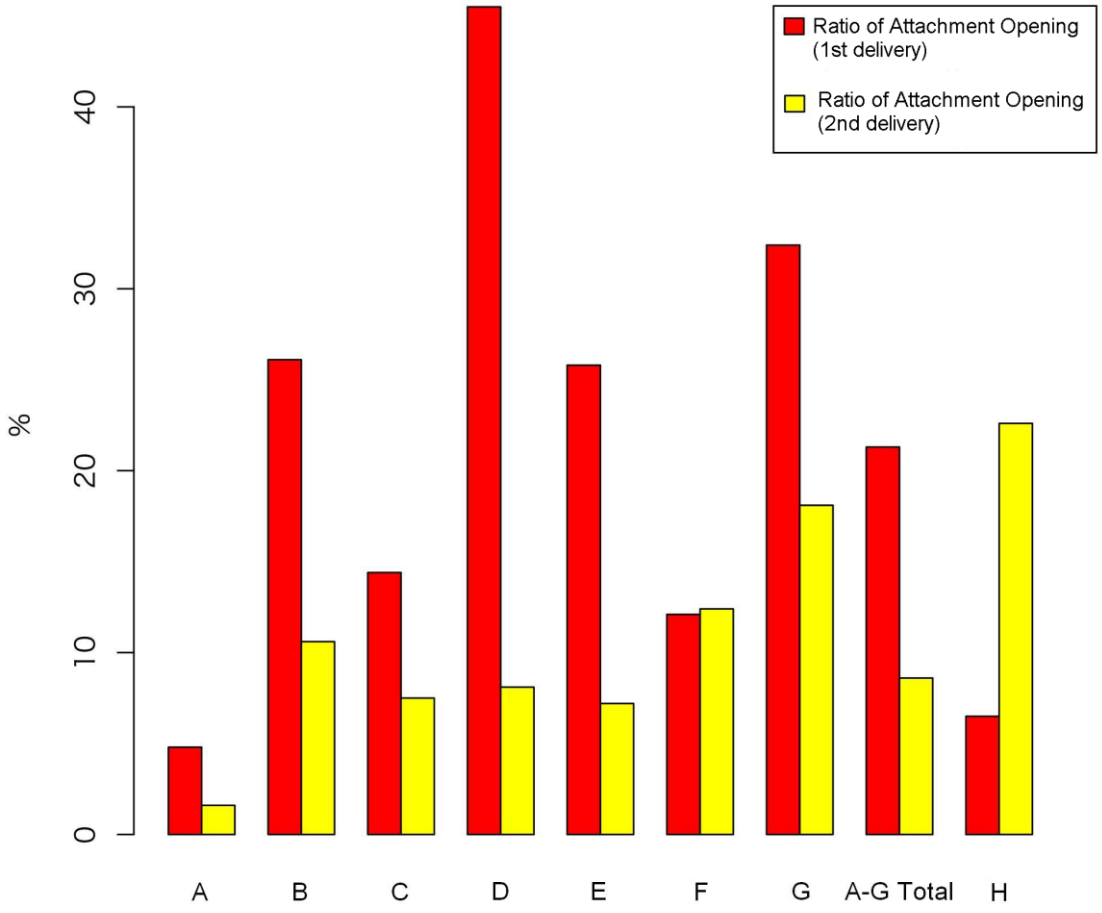
Subject Organization	Number of Participants	Pseudo-attack email		1st Delivery		2nd Delivery		Improvement Rate
		1st	2nd	Number of Participants who opened the Attachment	Ratio of Attachment Opening	Number of Participants who opened the Attachment	Ratio of Attachment Opening	
A	63	V	S	3	4.8%	1	1.6%	3.2%
B	161	S	T	42	26.1%	17	10.6%	15.5%

C	1,154	S	T	166	14.4%	87	7.5%	6.8%
D	198	V	W	90	45.5%	16	8.1%	37.4%
E	881	S	V	227	25.8%	63	7.2%	18.6%
F	282	S	U	34	12.1%	35	12.4%	-0.4%
G	188	S	T	61	32.4%	34	18.1%	14.4%
A-G Total	2927			623	21.3%	253	8.6%	12.6%
H	31	V	S	2	6.5%	7	22.6%	-16.1%
Total	2,958			625	21.1%	260	8.8%	12.3%
Total	2,958			625	21.1%	260	8.8%	12.3%

Fig. 3-2 is the Ratio of Attachment Opening at the 1st and 2nd deliveries, per Subject Organization represented as a graph.

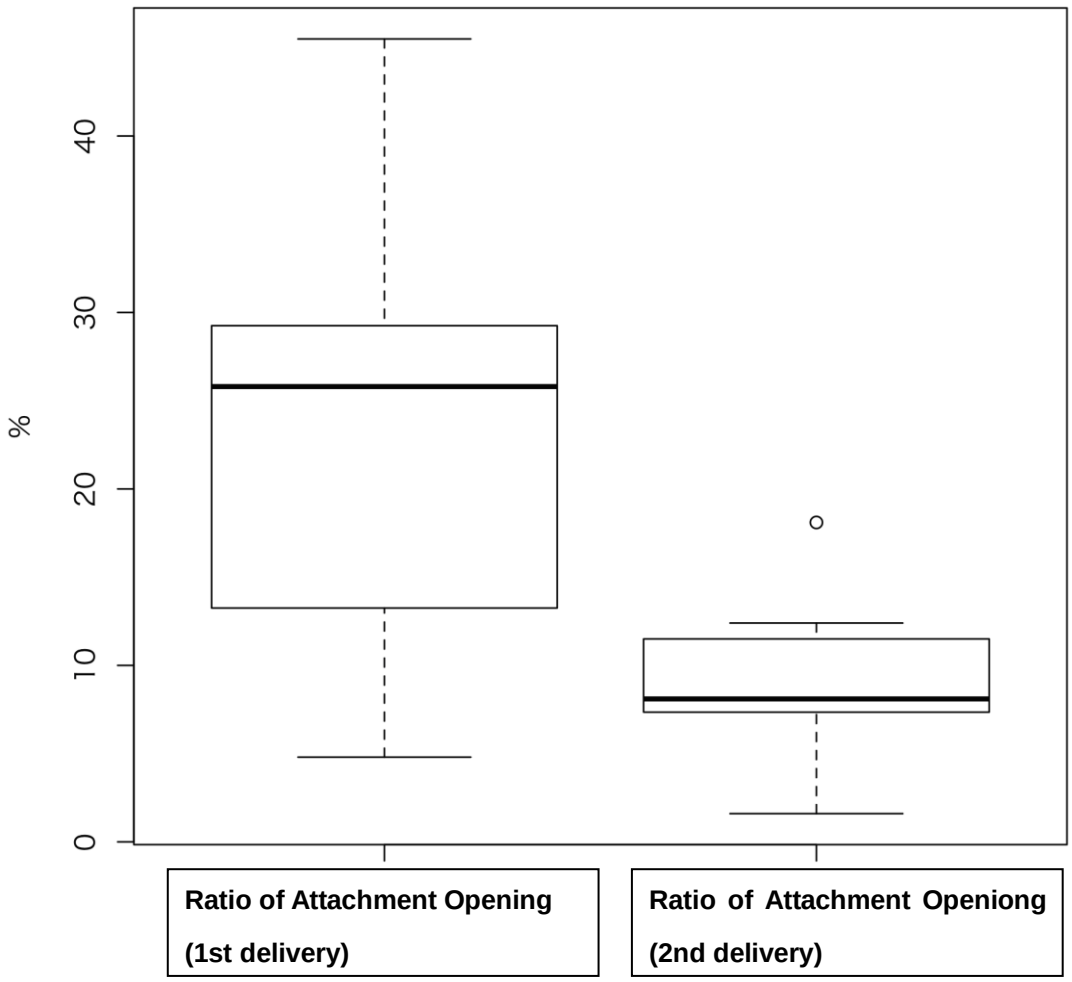
Except for Subject Organization F, in which the Ratios of Attachment Opening at the 1st and 2nd deliveries are roughly equivalent, you can see that for each Subject Organization, the ratios are lower at the 2nd delivery than at the 1st delivery. (As for Subject Organization H, numbers and graphs are shown as reference information. But those are not subject to consideration for the reason described in **2.11**. The same shall apply hereinafter.)

Fig. 3-2) Ratio of Attachment Opening per Subject Organization (1st and 2nd)



Also, a box-and-whisker plot for Organization A to G would be as shown in **Fig. 3-3**. Comparing the distribution of Ratio of Attachment Opened at the 1st delivery and that of the 2nd delivery using t-test, the p value is 0.02791 which means that there is “95% reliability of significant difference” between the two. That is, at the 2nd delivery, the education and training of the 1st delivery held 2 weeks ago turned to be effective, yielding a significant difference statistically.

Fig. 3-3) The Difference of the Ratio of Attachment Opening between Subject Organization A-G



In the box-and-whisker plot, the thick lines in the middle in vertical direction are the median value, and the upper and lower ends of the box shows the upper 25 percentile and the lower 25 percentile respectively. And the end point of the whisker extended from the boxes in horizontal direction shows the upper extreme value and the lower extreme value, respectively. And a circle symbol is plotted in the upper or lower direction of the box-and-whisker if there is an outlier.

By classifying the Attachment Opening Status of the Organizations into 4

categories, let us examine the log of the web beacon in more detail.

The first category is called “File-Openers 12”, which are participants who opened the attached files on both the 1st and the 2nd delivery. The second category is “File-Openers 1”, which are participants who opened the attached file on the 1st delivery, but not on the 2nd delivery. "File-Openers 2”, which are participants who did not open the attached file on the 1st delivery, but opened on the 2nd delivery. Finally, the participants, who did not open the attached file both on the 1st and the 2nd delivery, are called “Non-file-Openers”. These classified categories are tabulated in Fig**. 3-4**.

Fig. 3-4) 4 Categories of the File Openers

	1st Delivery	2nd Delivery
File-Openers 12	Opened	Opened
File-Openers 1	Opened	Not-opened
File-Openers 2	Not-opened	Opened
Non-file-openers	Not-opened	Not-opened

The count up based on this category is shown in
Fig. 3-5. Here, “Rate of Learning Effect” indicates the ratio of the File-Openers 1 to the Number of Participants who opened the attachment on the 1st delivery.

(Rate of Learning Effect) = (File-Openers 1) / (Number of Participants who opened the attachment on the 1st delivery)

The Rate of Learning Effect shows what percentage of Participants of the File-Openers on 1st delivery “learned” and refrained from opening files on the 2nd delivery. Basically, a higher Learning Effect is desirable.

Fig. 3-5) The Attachment Opening Status and the Rate of Learning Effect as seen from the Web Beacon logs

Subject Organization	File-Openers 12		File-Openers 1		File-Openers 2		Non-file-openers		Rate of Learning Effect
	Number of Participants	Ratio	Number of Participants	Ratio	Number of Participants	Ratio	Number of Participants	Ratio	
A	0	0.0%	3	4.8%	1	1.6%	59	93.7%	100.0%
B	6	3.7%	36	22.4%	11	6.8%	108	67.1%	85.7%
C	23	2.0%	143	12.4%	64	5.5%	924	80.1%	86.1%
D	10	5.1%	80	40.4%	6	3.0%	102	51.5%	88.9%
E	26	3.0%	201	22.8%	37	4.2%	617	70.0%	88.5%
F	3	1.1%	31	11.0%	32	11.3%	216	76.6%	91.2%
G	12	6.4%	49	26.1%	22	11.7%	105	55.9%	80.3%
A-G Total	80	2.7%	543	18.6%	173	5.9%	2131	72.8%	87.2%
H	0	0.0%	2	6.5%	7	22.6%	22	71.0%	100.0%
Total	80	2.7%	545	18.4%	180	6.1%	2153	72.8%	87.2%

The ratio of File-Openers per 4-Categories is depicted in a graph **Fig. 3-6**.

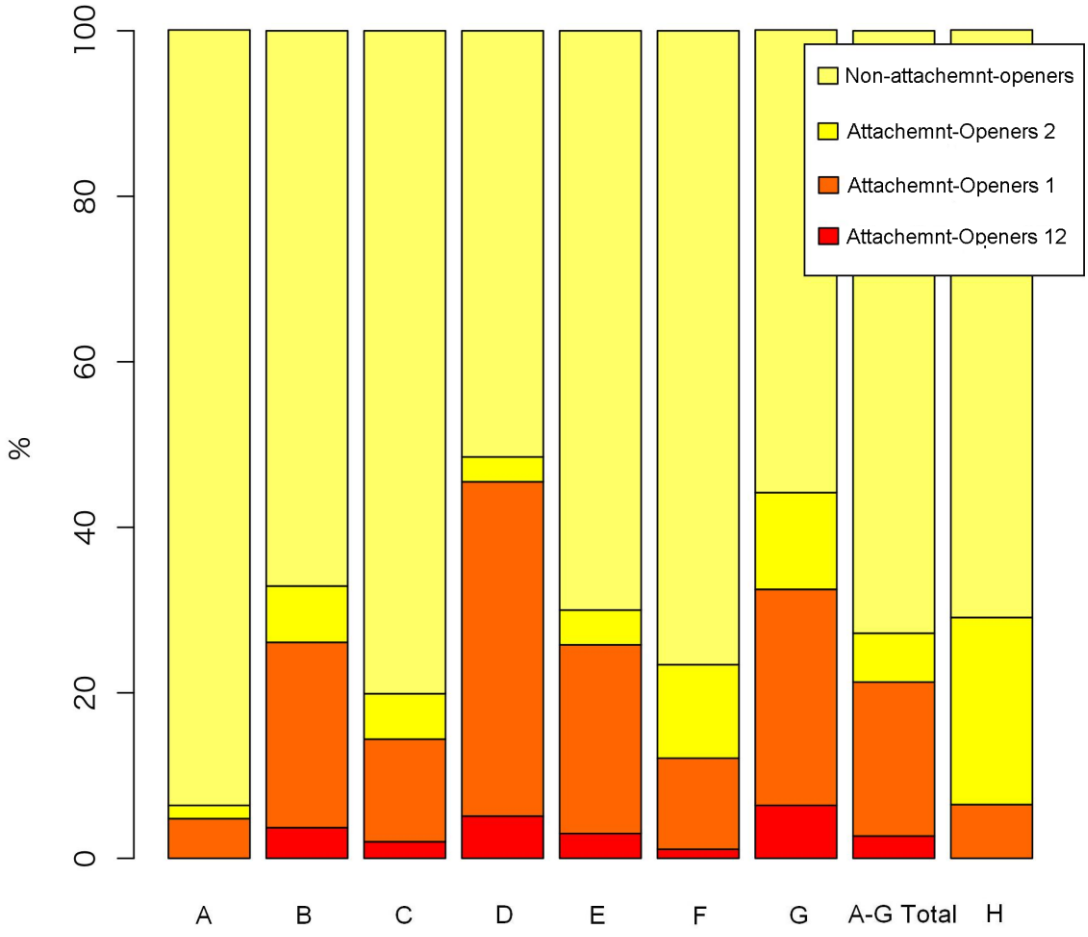
It is probably safe to say that the higher the percentage of Non-file-openers, the higher the resistance to targeted email attacks as a whole.

The average ratio of Non-file-openers is 72.8% in Subject Organizations A-G. From this, you can say that the Subject Organizations A and Subject Organizations C have a high resistance to targeted email attacks. On the other hand, the percentages of Non-file-openers in Subject Organizations D and G are low compared to the average. Therefore, at this point in time, you would have to say that the resistance of these organizations is low.

The higher the percentage of File-Openers 12, the more participants that are not aware of targeted email attacks, or dare to open attachments, even when they notice them. You can say this is a risk to the relevant Organizations.

From this viewpoint, Subject Organization G and D need to be careful.

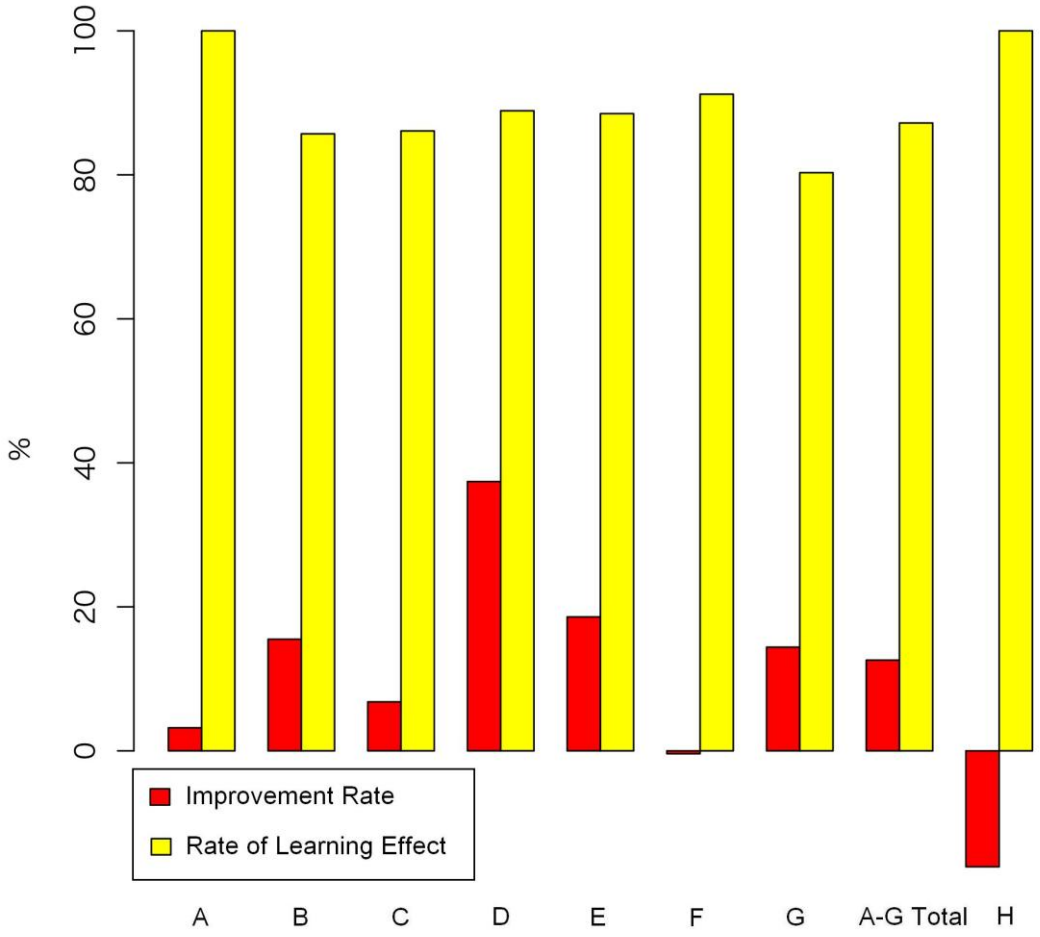
Fig. 3-6) 4-Categories of the Attachment Openers per Subject Organization



3.2 Improvement Rate and Rate of Learning Effect

Improvement Rate and Rate of Learning Effect per Subject Organization are depicted in a graph (**Fig. 3-7**).

Fig. 3-7) Improvement Rate and Rate of Learning Effect per Subject Organization



High Improvement Rate means that lessons learned on the 1st delivery proved effective on the 2nd delivery.

The results of this time show that the Improvement Rate of Organizations D, E, G, and B are large, and that of Organization F is small.

However, since the type of pseudo-attack email used on the 1st delivery differs from the one used on the 2nd delivery, when the pseudo-attack email on the 2nd delivery is extremely “persuasive (strong) in leading to opening”, the

Improvement Rate will appear low. It will depend on individual situations, but assuming from what we have heard from the person in charge at Subject Organizations F, it seems highly possible that the pseudo-attack email used on the 2nd delivery at Organization F was “strong”.

The low Improvement Rate in Subject Organization A, which has a high Non-file-opener ratio, may have resulted from the fact that while the Ratio of Attachment Opening remains low to the utmost limit, incidental file openers appeared. Since the overlap would be small between the number of Participants who opened the attachment on the 1st and the 2nd deliveries, and the numbers did not vary much, the Improvement Rate will be low. The Improvement Rate is expected to transit from “Middle -> High -> Low” as education and training such as inoculation are conducted.

As for the Rate of Learning Effect, all subject organizations showed a high level. One can see that lessons learned from opening the attachment on the 1st delivery have been put into practice effectively on the 2nd delivery performed two weeks later. Some Subject Organizations accomplished the Rate of Learning Effect of 100%. So, by implementing education/training, the Rate of Learning Effect may transition from “Middle” or “Large” to “100”.

This means that the effect of inoculation remains effective for at least 2 weeks, and this matches the fact that there was a significant difference between the Ratio of Attachment Opening on the 1st and 2nd delivery.

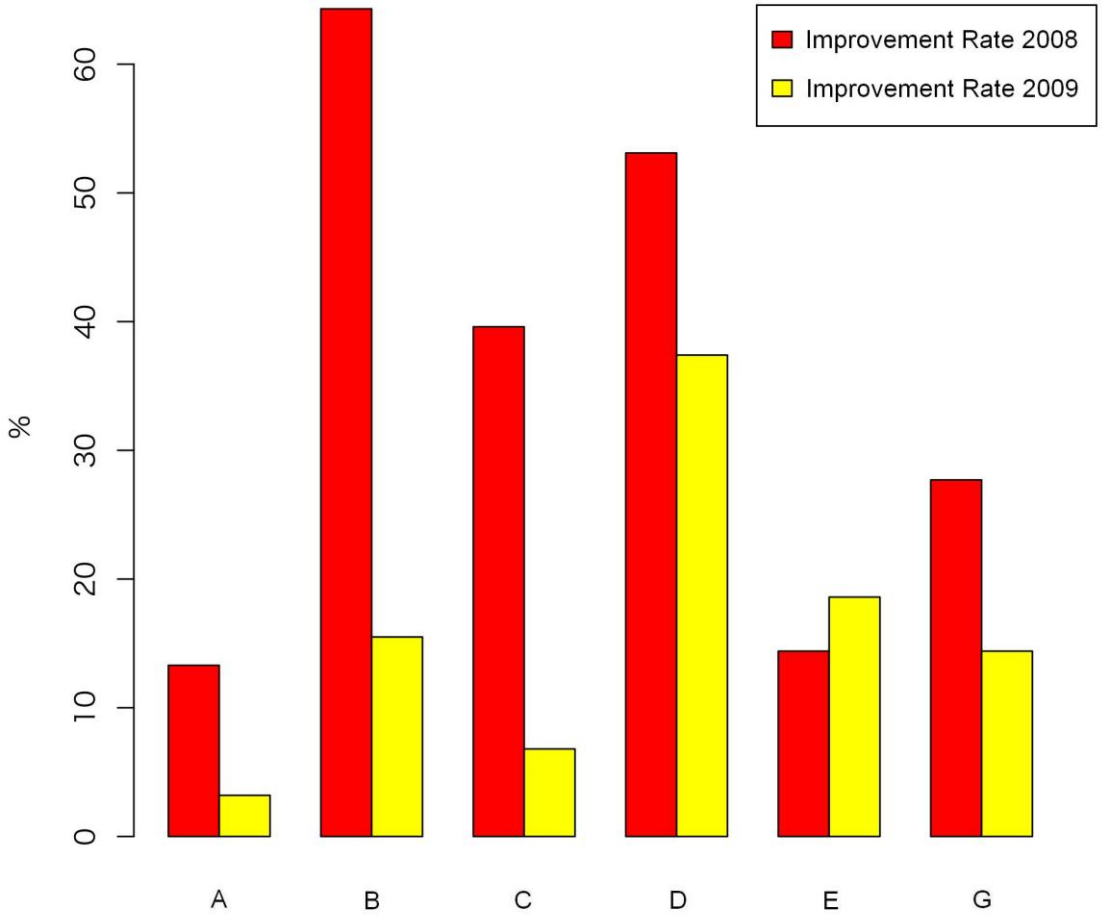
3.3 Transition of Improvement Rate, the Rate of Learning Effect, Non-File-Opener Rate over Time

Here, we compare the Improvement Rate, the Rate of Learning Effect, Non-File-Opener Rate in last fiscal year (2008) and this fiscal year (2009) for comparable Subject Organizations (A to E, and G).

First, the Improvement Rate is shown in **Fig. 3-8**. (The data of the last fiscal year

(2008) are obtained from the reports of that year. The same shall apply hereinafter.)

Fig. 3-8) Transition of Improvement Rate Over Time



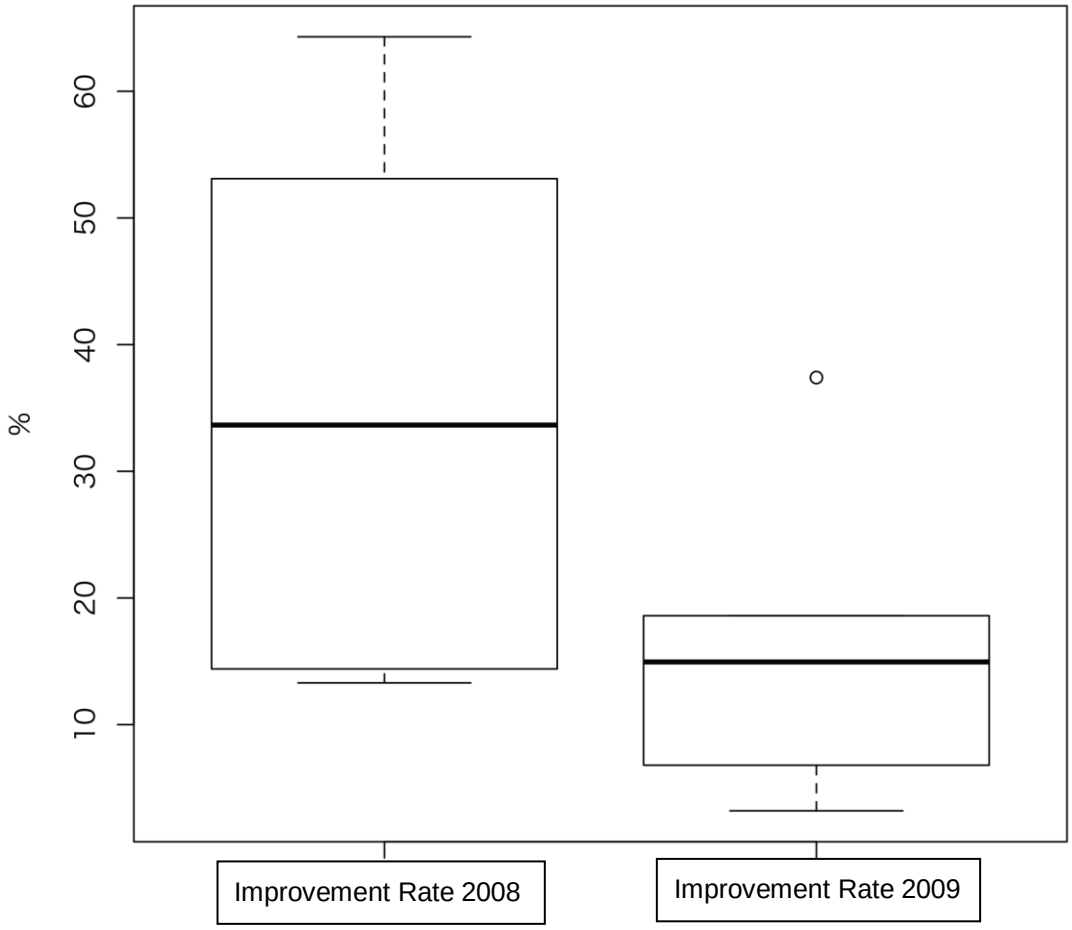
The Improvement Rates have declined in all Subject Organizations, except for Organization E. The inoculation (as well as education/training and news etc. of informational security in general) seems to have been effective.

With regard to Subject Organization E, the result seems to reflect strong characteristics of the initial stages of education and training since the number of

participants were significantly increased compared to the last fiscal year (2008).

Data for each subject organization per year are shown in the box-and-whisker plot (**Fig. 3-9**).

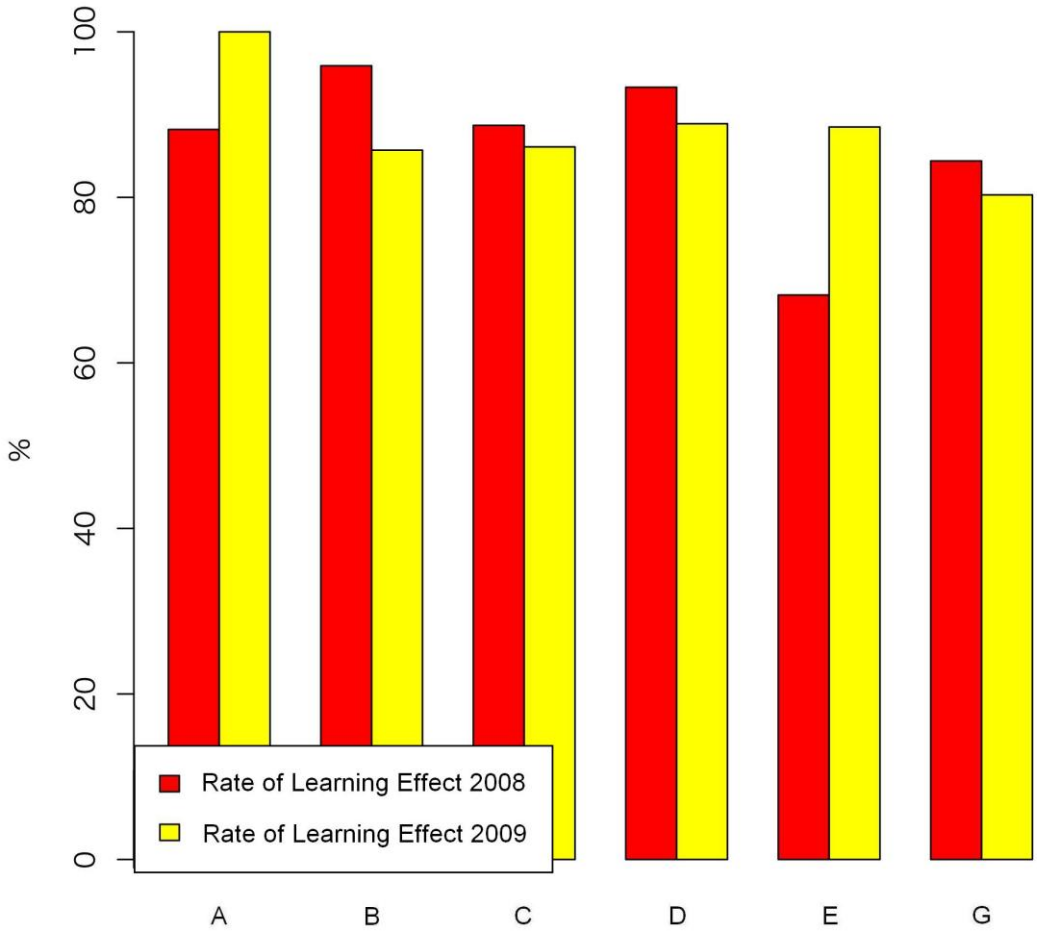
Fig. 3-9) Transition of Improvement Rate Over Time (Box-and-Whisker Plot)



By performing a t-test for the distribution of Improvement Rates of the last fiscal year (2008) and this year (2009), the p-value is 0.05122, which means there is 90% reliability of significant difference between the two. That is to say, the Improvement Rate is certainly declining.

Next, the transition of The Rate of Learning Effect of both years is shown in **Fig. 3-10**.

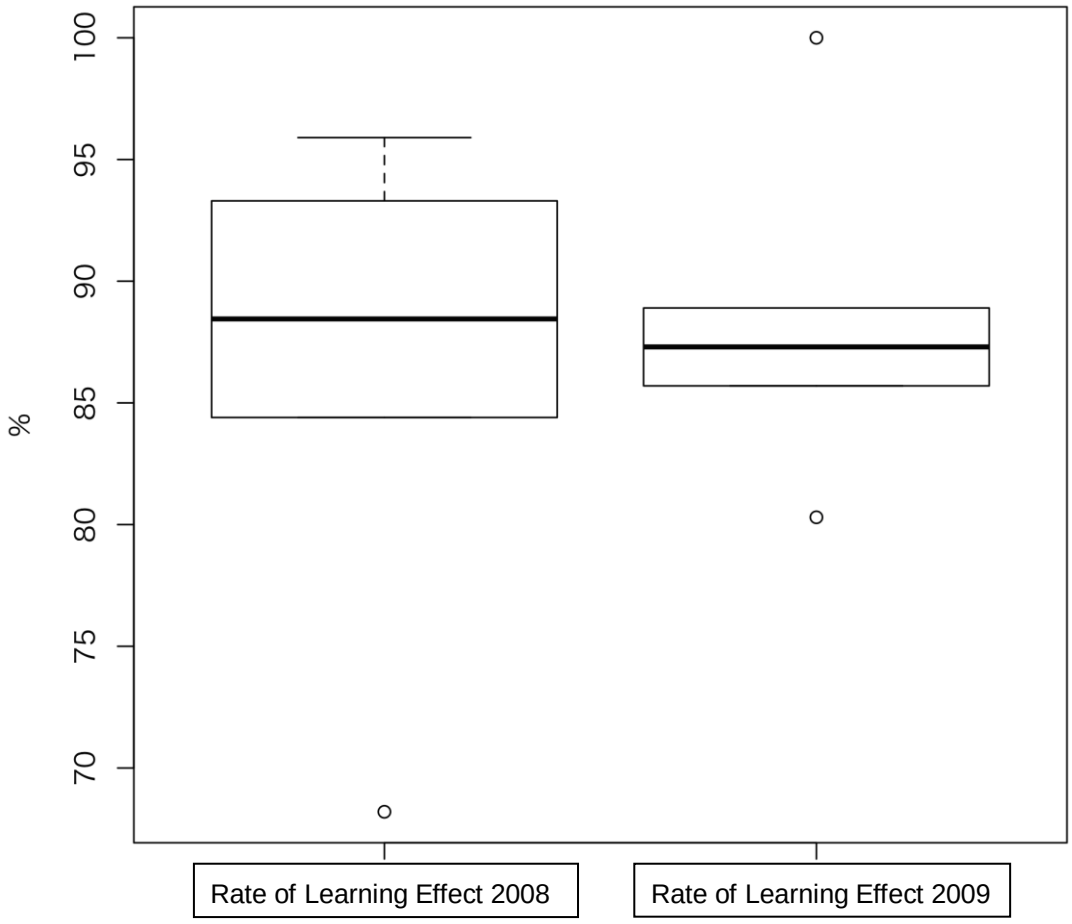
Fig. 3-10) Transition of Rate of Learning Effect Over Time



By comparing the transition of Rate of Learning Effect over time, some Subject Organizations had a rather low percentage in the last fiscal year (2008), but most have accomplished a high level of 80% this fiscal year (2009). Here also, you can say that the effect of inoculation remains effective for at least 2 weeks.

This is shown as the box-and-whisker plot in. **Fig. 3-11**.

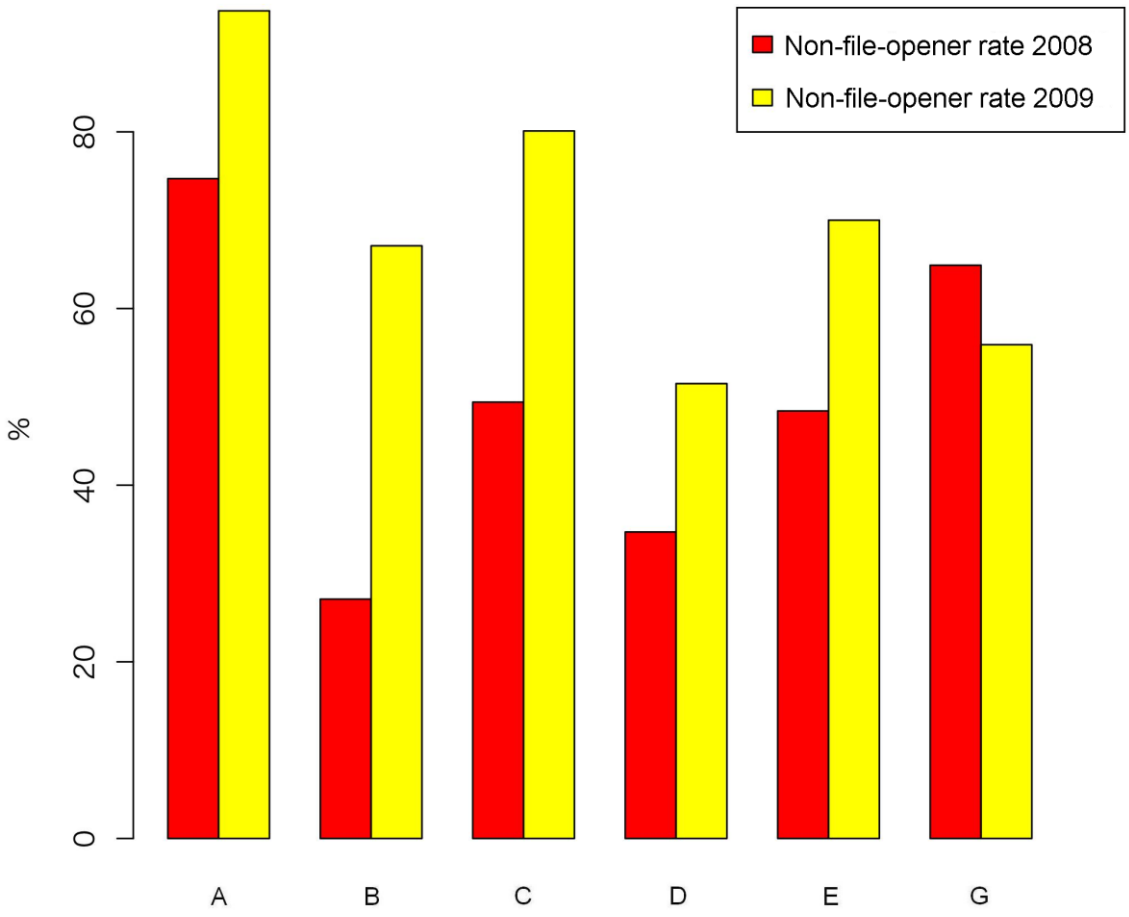
Fig. 3-11) Transition of Rate of Learning Effect Over Time (Box-and-Whisker Plot)



You may intuitively notice that there is no obvious change in the Rate of Learning Effect in the box-and-whisker plot. Also, the p-value is 0.7207 indicating that there is no significant difference.

Next, the transition of the Non-file-opener rates over time is depicted in graph. **Fig. 3-12**.

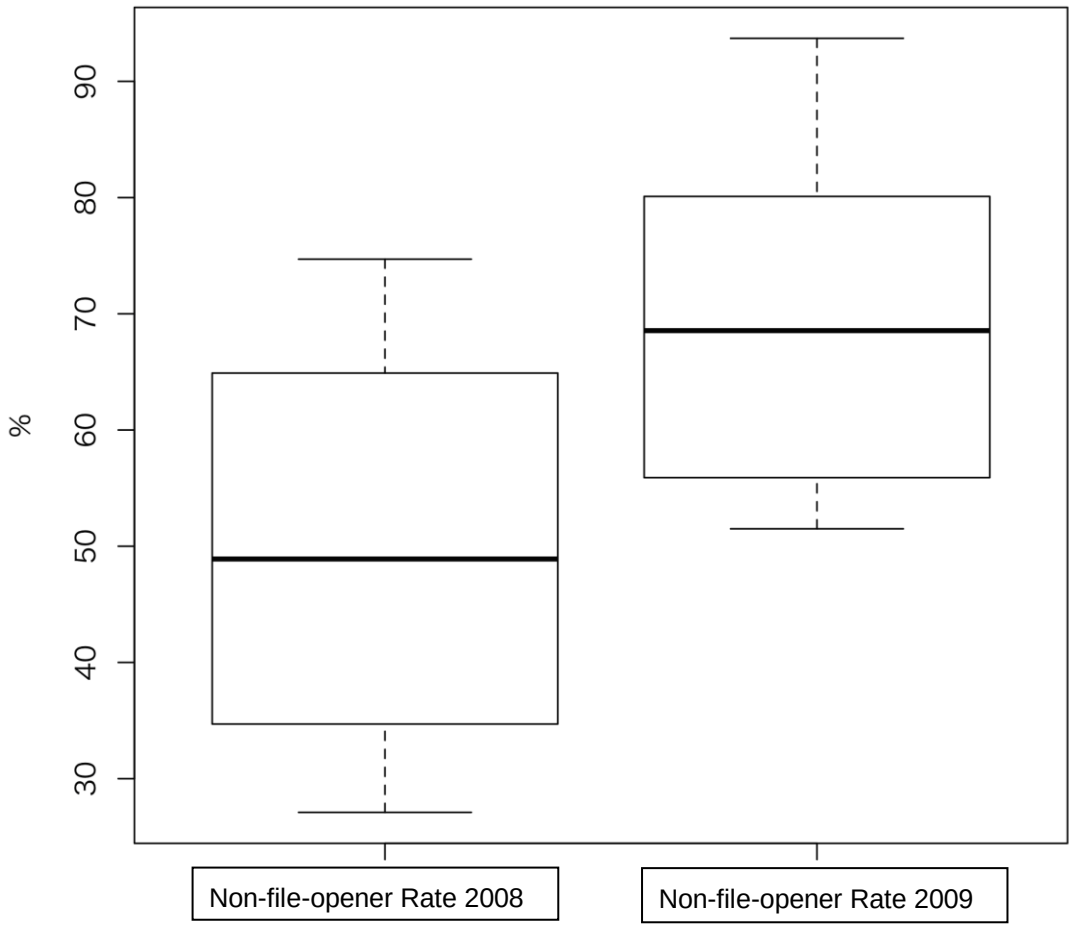
Fig. 3-12) Transition of Non-File-Opener Rate Over Time



In the Transition of Non-File-Opener Rate Over Time, except for Subject Organization G, the Non-File-Opener Rate is higher this fiscal year (2009) than last year (2008). As an overall organization, it seems that they have successfully acquired resistance against targeted email attack.

To verify this, the box-and-whisker plot is depicted as the graph in **Fig. 3-13**.
The p value is 0.03232, and therefore there is 95% reliability that the Non-File-Opener Rate is increasing.

Fig. 3-13) Transition of Non-File-Opener Rate Over Time (Box-and-Whisker Plot)



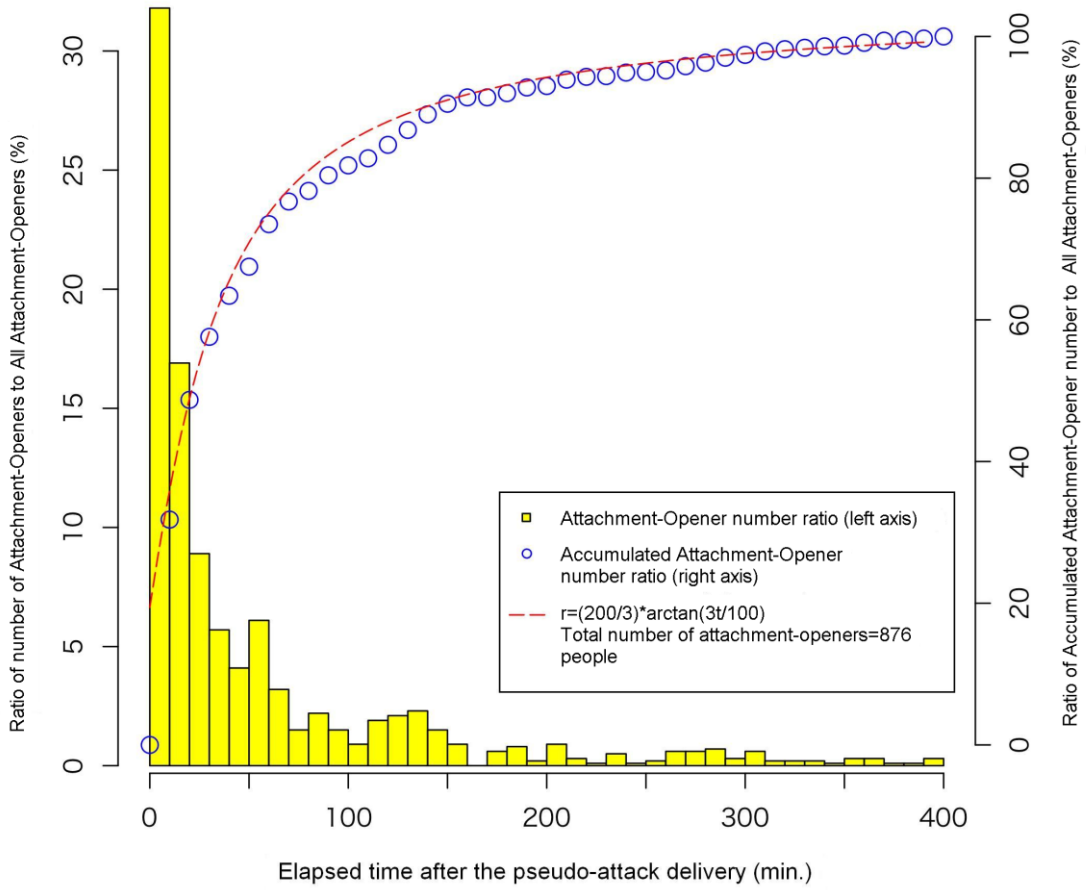
3.4 Attachment Opening Status as seen from Web Beacon

Looking from a different angle, let us analyze the Web beacon log and view the trend of elapsed time in minutes since the pseudo-attack email is delivered, up until the time a File Opener actually opens an attachment.

In our observation gained in the last fiscal year (2008), the largest number of file openers opened the attachment just after pseudo-attack email delivery, and the number rapidly declined as time elapsed. Similar tendency can be seen this year (2009). A chronologically ordered graph which uses the data of this year (2009)

is depicted in **Fig. 3-14**.

Fig. 3-14) Attachment Opening Status Monitored by Web Beacon



This graph was produced by creating a histogram of every 10 minutes (yellow vertical bar, left axis) by extracting each Participant's file-opening time from the web beacon log of Subject Organizations A-G at the 1st and 2nd delivery. Also, the accumulated total are plotted (blue circle, right axis), and a curve is applied to the plotted line using a function (red dotted line, right axis). With regard to Subject Organizations A-G of this research, a total of 876 File-Opening events have occurred, and the ratio to the total numbers of File Openers (876 people) are used for the vertical axis.

When applying a function to the File-Openers ratio, we found it matches well with the following formula.

$$r = (200 / 3) * \arctan(3 * t / 100)$$

r：Ratio of the Opened File to the Total File Openers (%)

t：Elapsed time after Pseudo-Attack Email Delivery (min.)

From this function application, for half an hour after the pseudo-attack email delivery, you can see that half of the file-openers have already opened the files. That is, if this kind of targeted email attack occurs, much of the direct damages occur just after the attacks. This should be considered when taking measures.

The Ratio of Attachment Opening of Subject Organizations A-G at 1st delivery is 21.8% in average. If you assume this is general, we can argue the following.

That is, if a pseudo-attack email is delivered to 100 participants, about 22 participants would open the attached file. 11 people, which is about half the number of the 22 File Openers, will probably open the file within 30 minutes after pseudo-attack email delivery.

3.5 The “Strength” of the Six Types of Pseudo-Attack Emails

In this research, we prepared six types of pseudo-attack email (body, subject) as shown in **Fig.2-5** and after. And we have already mentioned that each Subject Organization selected two types out of the six as the pseudo-attack email to be sent out on each delivery. The result of the selection is shown in **Fig. 3-1**.

Here, if a pseudo-attack email has a tendency to have a higher Ratio of Attachment Opening compared to other pseudo-attack mails, we can say that it is a “strong” pseudo-attack mail. Adversely, if pseudo-attack emails have strength levels, it may be possible to compare the Ratio of Attachment Opening between the different Inoculation attempts by adjusting the levels.
Therefore, we verified whether it is possible to identify such tendency from the results of this research.

In the 1st pseudo-attack email delivery (Subject Organizations A-G) of this research, pseudo-attack emails S and V were selected. Ratio of Attachment Opening of the 1st delivery per type of pseudo-attack email is plotted in **Fig. 3-15**.

Likewise, the ratio of the 2nd delivery is also plotted in the graph (**Fig. 3-16**). On the 2nd delivery, the relations to the pseudo-attack email types used on the 1st delivery may present a problem, but here, we just pick up the pseudo-attack email types on the 2nd delivery.

Unfortunately, we cannot identify any trends in these graphs. This may be because the number of examples is too small to show any trend or it may be that such tendency is originally a mere side effect and the difference of the Subject Organizations may be a main factor. Whatever the case, it is difficult to establish a hypothesis at this time, and this must be considered in the future.

Fig. 3-15) Pseudo-Attack Email Types and Ratio of Attachment Opening at 1st Delivery

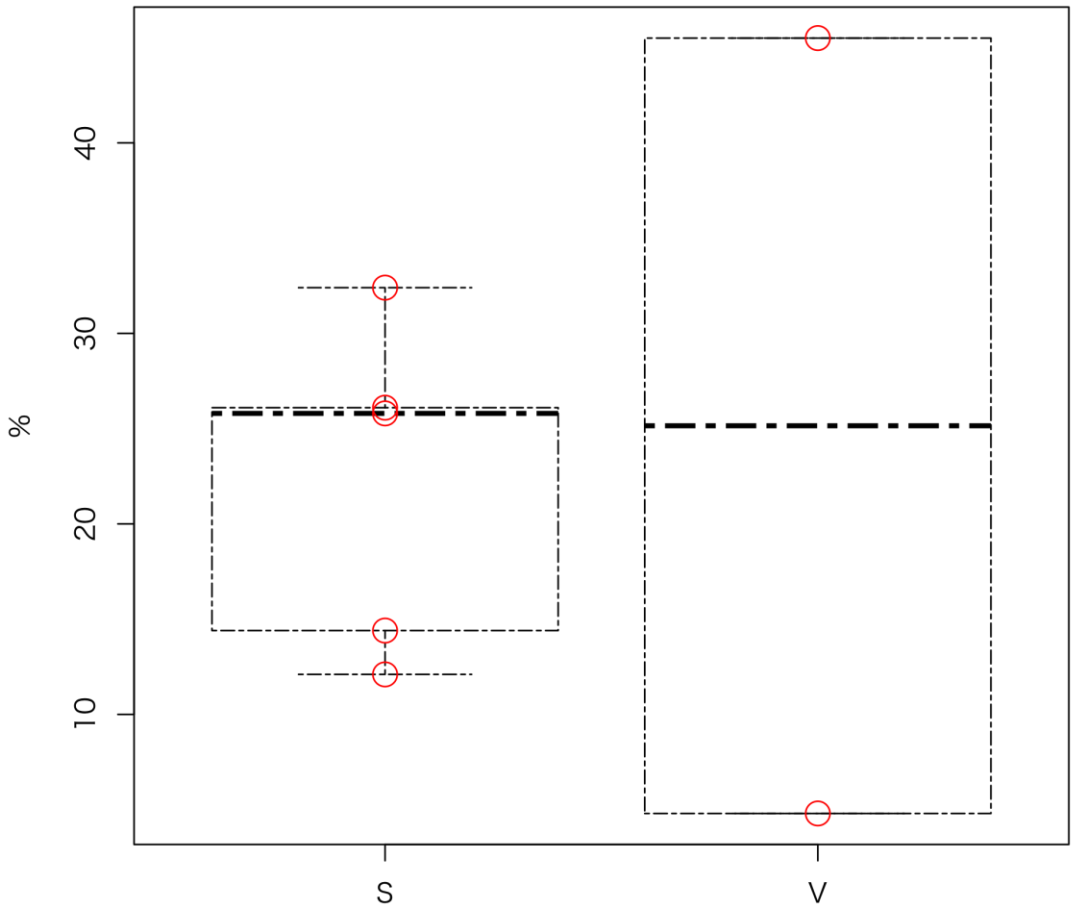
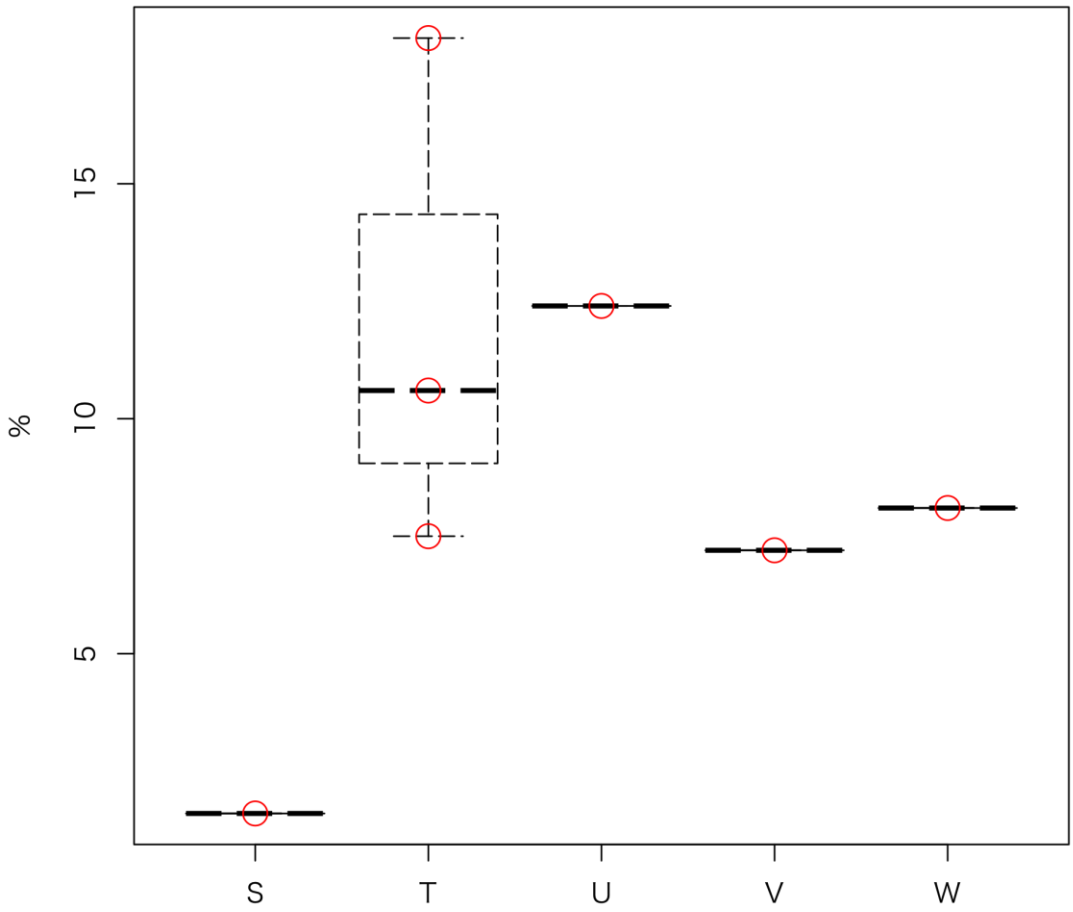


Fig. 3-16) Pseudo-Attack Email Types and Ratio of Attachment Opening at 2nd Delivery



4 Results of the Questionnaire

4.1 Response Rate of Questionnaire

First, the response rate of the questionnaire is shown in. **Fig. 4-1**. Though they vary depending on the Subject Organization, the response rate of each Subject Organization was 30% or over, and on average, the rate is 38.6%, which we assume that there is no problem with response rates.

Fig. 4-1) Response Rates of Questionnaire

Subject Organization	Number of Participants	Questionnaire	
		Number of responses	Response Rate
A	63	23	36.5%
B	161	63	39.1%
C	1,154	385	33.4%
D	198	109	55.1%
E	881	266	30.2%
F	282	210	74.5%
A-F Total	2,739	1056	38.6%
G	188	123	65.4%
H	31	14	45.2%
Total	2,958	1,193	40.3%

4.2 Profiles of the Subject Organizations

By summarizing the results of the questionnaire, property information is shown in graph form such as **Fig. 4-2** , which depicts gender, **Fig. 4-3** , which depicts age-group, **Fig. 4-4** depicts types of duties, **Fig. 4-5** , which depicts mail proficiency, by Subject Organizations.

As for gender, it consists mainly of men. As for age-group, there are few people below the age of 20, and it consists mainly of people in their 20’s to 40’s. As for

duties, while it depends on the Subject Organization, it is divided roughly into three positions: managerial, clerical, and technical positions. As for email proficiency, most participants evaluate their proficiency as average level, or above.

Fig. 4-2) Gender Ratio per Subject Organization Derived from Questionnaire

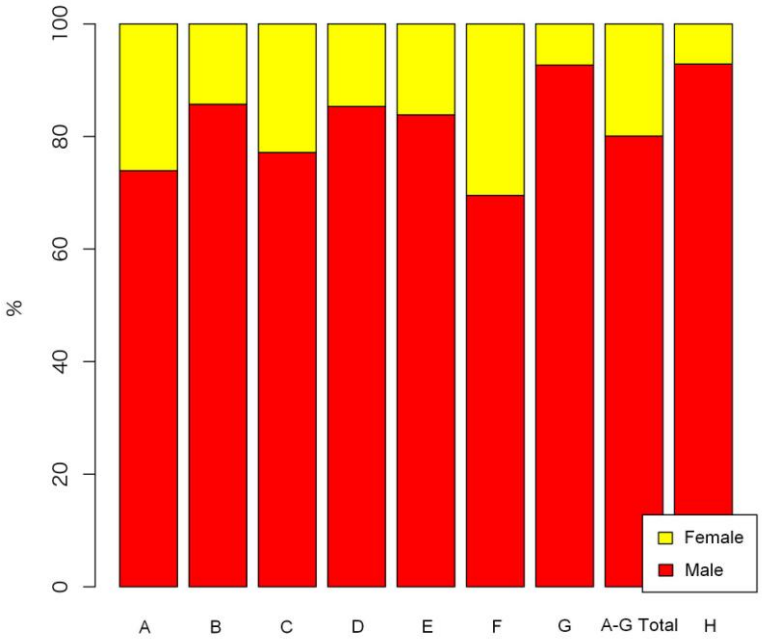


Fig. 4-3) Age-Group Ratio per Subject Organization Derived from Questionnaire

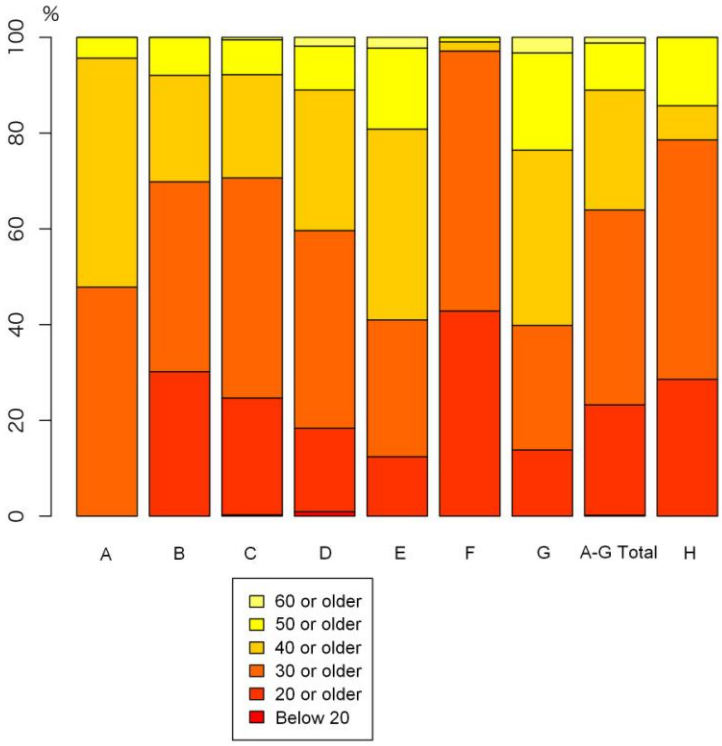


Fig. 4-4) Ratio of Job Roles per Subject Organization Derived from Questionnaire

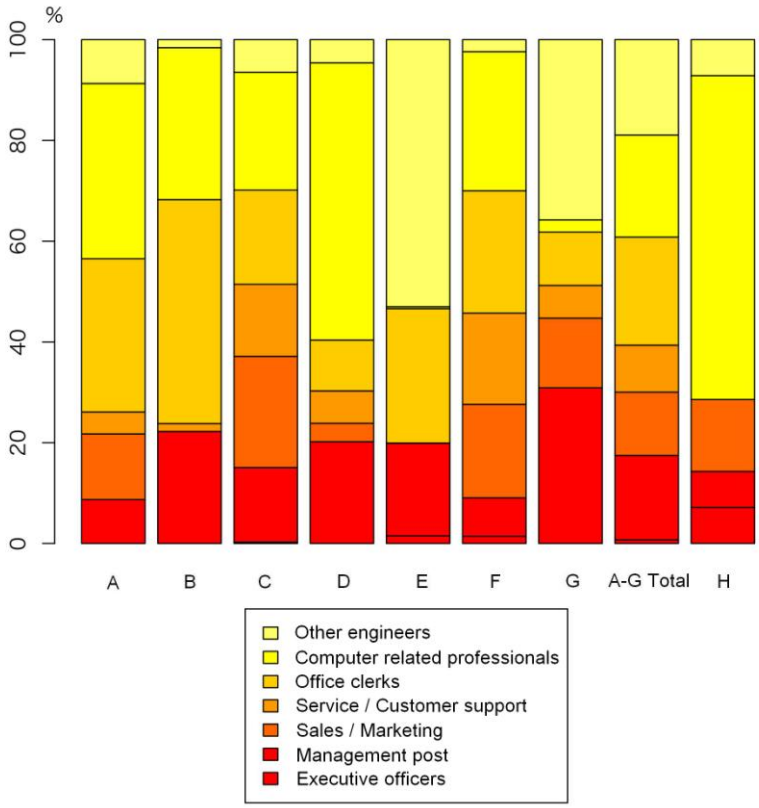
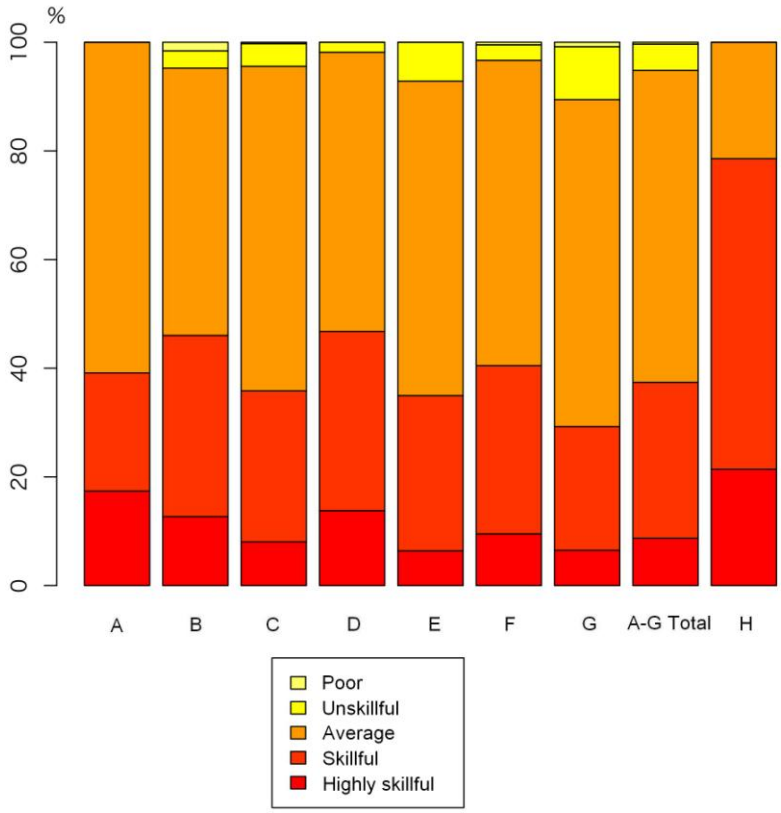


Fig. 4-5) Ratio of Mail Proficiency per Subject Organization Derived from Questionnaire



4.3 Attachment Opening Status Summarized from Questionnaire

By summarizing the answers of the questionnaire, we created tables corresponding to **Fig. 3-1** and
Fig. 3-5. If the Attachment Opening Status as seen from the results of the questionnaire has a strong resemblance with the one seen from the web beacon, it would be a good reason to adopt the results obtained from the analysis of the questionnaire.

First, the Number of Participants who opened the Attachment / Ratio of Attachment Opening of each delivery and improvement rate are shown in. **Fig. 4-6**.

Fig. 4-6) Data of Examinee Questionnaires and Improved Rate

Subject Organization	Number of respondents	1st Delivery		2nd Delivery		Improved rate
		Number of Participants who opened the	Ratio of Attachment Opening	Number of Participants who opened the	Ratio of Attachment Opening	
A	22	3	13.6%	0	0.0%	13.6%
B	63	11	17.5%	4	6.3%	11.1%
C	368	50	13.6%	32	8.7%	4.9%
D	105	53	50.5%	10	9.5%	41.0%
E	252	72	28.6%	10	4.0%	24.6%
F	196	51	26.0%	30	15.3%	10.7%
A-F Total	1006	240	23.9%	86	8.5%	15.3%
H	13	0	0.0%	3	23.1%	-23.1%

Also, the Attachment Opening Status and the Rate of Learning Effect summarized from the questionnaires are shown in **Fig. 4-7**.

Fig. 4-7) Attachment Opening Status and Rate of Learning Effect as seen from Questionnaire

Subject Organization	File-Openers 12		File-Openers 1		File-Openers 2		Non-file-openers		**Rate of Learning Effect**
	Number of Participants	Ratio	Number of Participants	Ratio	Number of Participants	Ratio	Number of Participants	Ratio	
A	0	0.0%	3	13.6 %	0	0.0%	19	86.4 %	0.0%
B	3	4.8%	8	12.7 %	1	1.6%	51	81.0 %	4.8%

C	12	3.3%	38	10.3 %	20	5.4%	298	81.0 %	3.3%
D	5	4.8%	48	45.7 %	5	4.8%	47	44.8 %	4.8%
E	8	3.2%	64	25.4 %	2	0.8%	178	70.6 %	3.2%
F	17	8.7%	34	17.3 %	13	6.6%	132	67.3 %	8.7%
A-F Total	45	4.5%	195	19.4 %	41	4.1%	725	72.1 %	4.5%
H	0	0.0%	0	0.0%	3	23.1 %	10	76.9 %	0.0%

Based on these tables, graphs, which correspond to **Fig. 3-2** and **Fig. 3-6** , are depicted in エラー**!** ブックマークが自己参照を行っています。 and **Fig. 4-9**.

As these graphs look much alike each other, it seems that they show a pattern similar with the Attachment Opening Status as seen from the web beacon. Therefore, if answers related to the Participants' various properties are analyzed in conjunction with the Attachment Opening Status, it would considerably match the overall picture of the Participants.

Fig. 4-8) Ratio of Attachment Opening per Subject Organization (1st and 2nd deliveries)

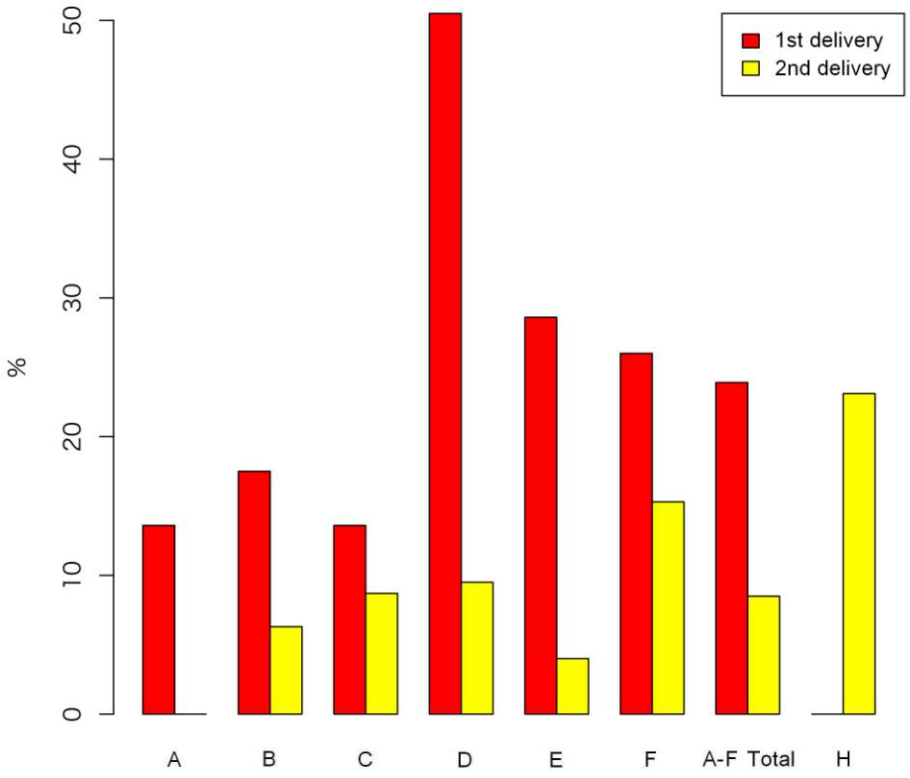
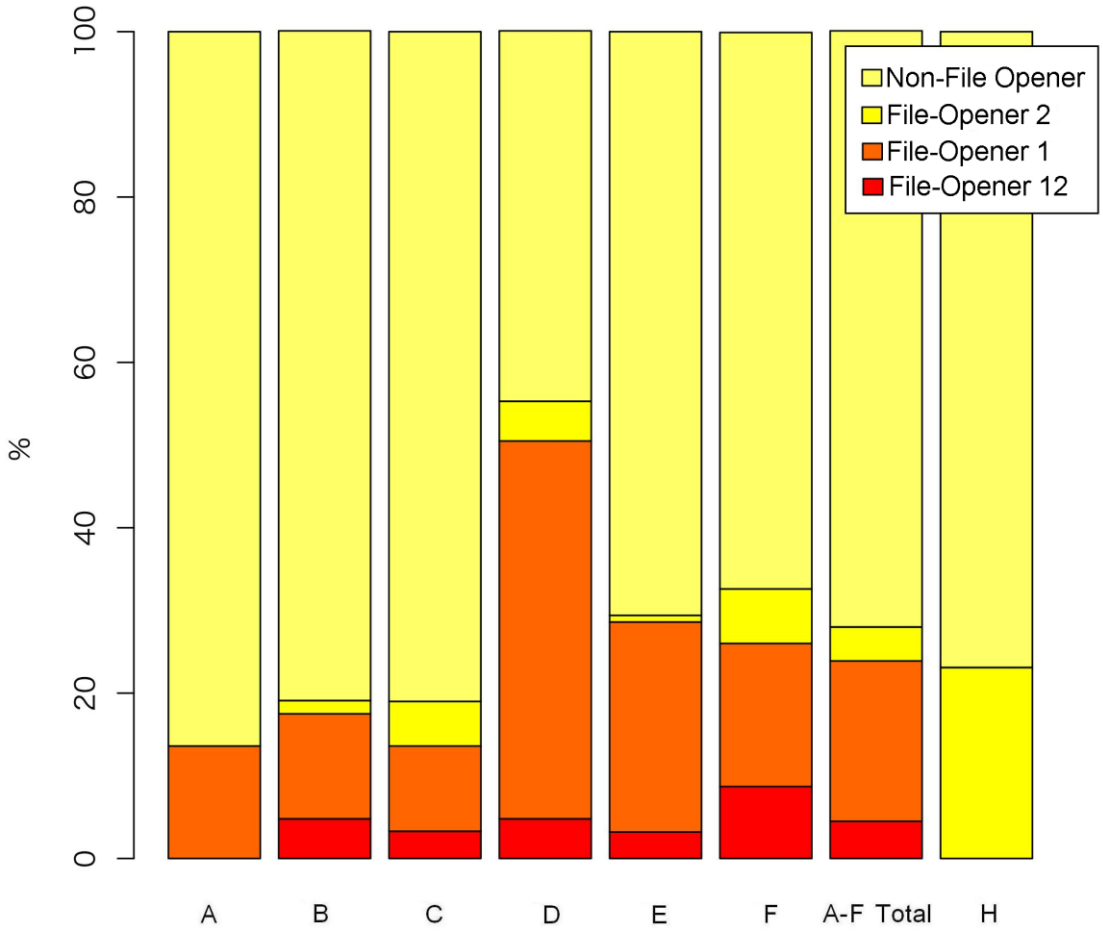


Fig. 4-9) Ratio among the Four Categories of File Openers per Subject Organization



4.4 Risk Group Hypothesis Verification

By counting up the number of file openers / non-file openers on each delivery per selection option of the questionnaire, their correlation is depicted in **Fig. 4-10**.

The p values in the table are basically from Fisher-tests, and for cases where Fisher-tests are not applicable, Chi-square tests were applied. As a result, options with a 95% reliability that there is a significant difference between them

were Email Proficiency, Number of Mails (per 1 day/in average), Number of Processed Mails (per one email process hour), With or Without Experience of Inoculation, Relevancy to Work (of pseudo-attack email body, subject). These are highlighted in light green.

You can see that there is virtually no correlation between the properties such as gender, age group, duties and the Open and Non-open of files, which is comparable with the observations obtained last (2008) year.

Some property shows significant difference in the Ratio of Attachment Opening on 1st delivery, but some of the properties, such correlation cannot be found in the Ratio of Attachment Opening on 2nd delivery.

Fig. 4-10) Properties and the p Values of Attachment Opening Status as Seen from Questionnaire

Question	Options	1st Delivery			2nd Delivery		
		Opened	Not-opened	p value	Opened	Not-opened	p value
Gender	Male	198	622	0.3261	69	752	0.2298
	Female	46	174		24	193	
Age group	Under 20	1	0	0.1394	0	2	0.436
	In their 20's	60	194		24	229	
	In their 30's	104	341		35	407	
	In their 40's	52	189		20	221	
	In their 50's	22	68		13	77	
	60 or above	5	4		1	9	
Duty	Executive officers	2	6	0.2789*	2	6	0.4402*
	Management post	36	120		15	141	
	Sales / Marketing	25	104		13	115	

	Service / Customer support	16	80		6	94	
	Office clerks	53	183		24	212	
	Computer related professionals	61	179		22	214	
	Other engineers	51	124		11	163	
mail proficiency	Highly skillful	23	72	0.009841	10	85	0.0006635
	Skillful	66	245		22	288	
	Average	136	452		51	537	
	Unskillful	16	27		7	35	
	Poor	3	0		3	0	
Number of mails	Less than 25/day	111	245	0.0002386	30	325	0.3122
	25 – less than 100	70	255		25	299	
	100 – less than 250	46	205		30	221	
	250 and above	17	91		8	100	
Total email process time	Less than 2 hours/day	141	404	0.1619	45	498	0.5005
	2 – less than 4	86	323		38	372	
	4 and above	17	69		10	75	
Number of email processed per 1 hour	Less than 25/hour	137	352	0.004046	41	444	0.5751
	25 – less than 100	71	269		32	310	
	100 – less than 250	25	115		16	123	

	250 and above	9	59		4	64	
With or without experience of Inoculation Program	Experienced	74	405	1.351e-08	29	444	0.004344
	Not experienced	170	391		64	501	
Relevancy to Work	Very much related	42	67	3.637e-05	24	103	2.027e-05
	Much related	78	263		35	300	
	Slightly related	46	242		13	301	
	Not related	78	224		21	241	

Below, we consider each property which had significant differences:

As for email proficiency, the Ratio of Attachment Opening is highest in the groups who answered “Poor”, as in **Fig. 4-11** or **Fig. 4-12**. A hypothesis that this group is most likely the risk groups, is natural, but the possibility that the fact that they have opened the file makes them think themselves as “Poor” cannot be dismissed.

Fig. 4-11) Email Proficiency and the Attachment Opening Status at 1st Delivery

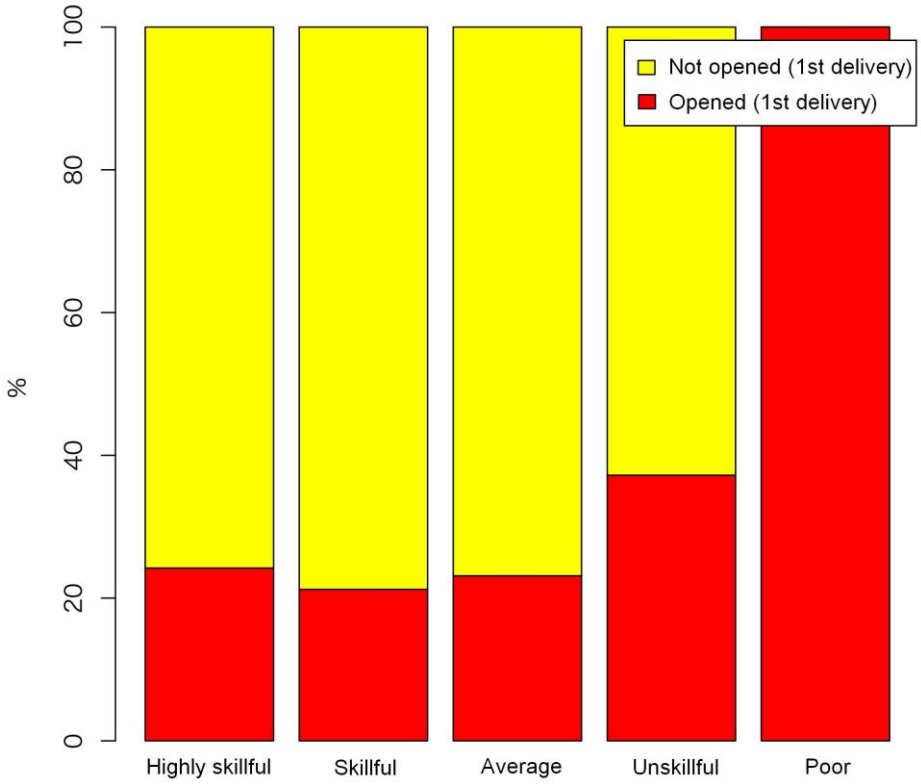
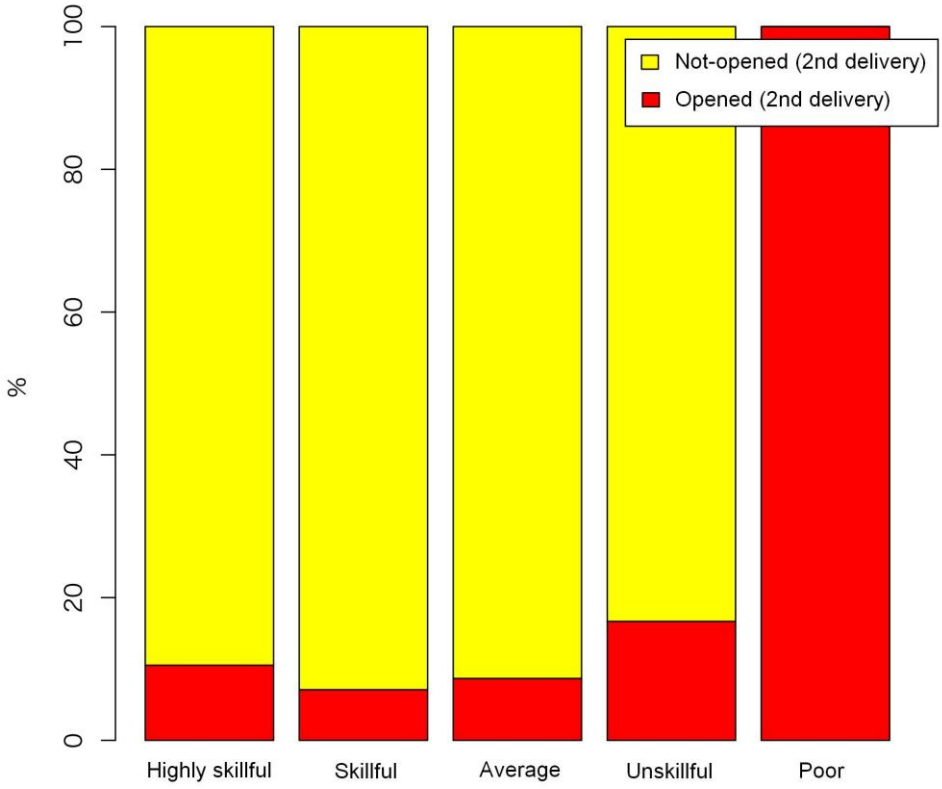


Fig. 4-12) Email Proficiency and Attachment Opening Status at 2nd Delivery

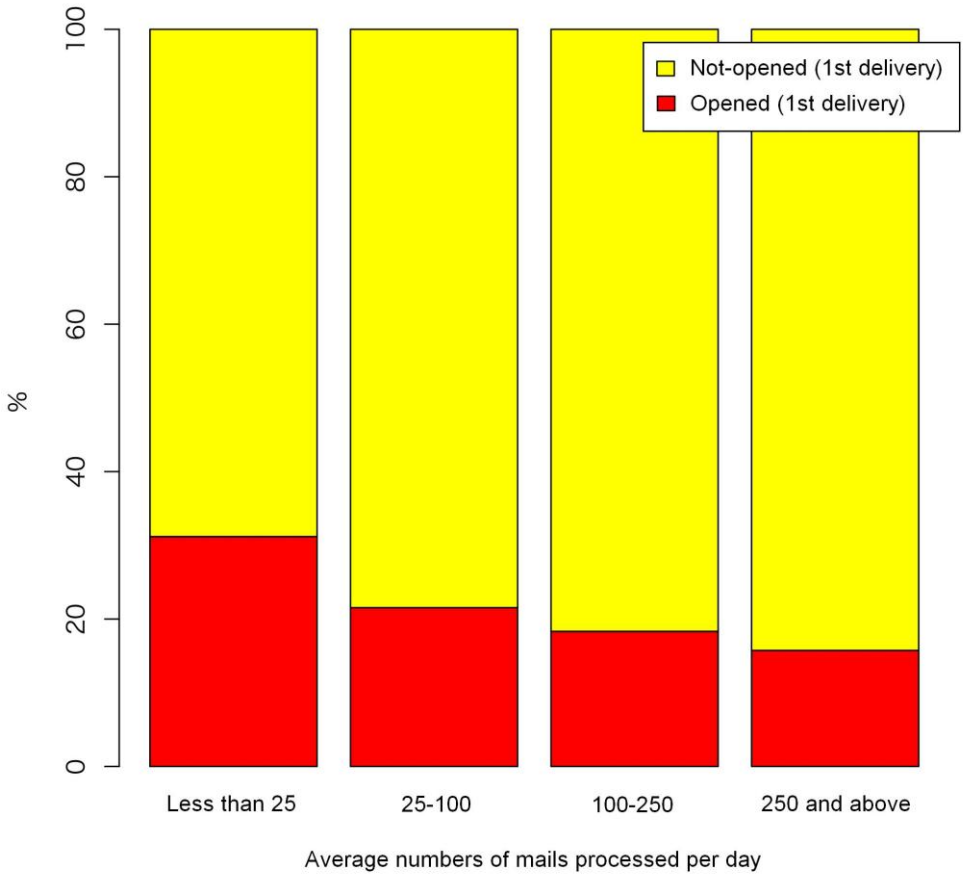


Next, as for Number of Email per Day, **Fig. 4-13** shows that the smaller the number of emails per day, the more the numbers of File-Openers.

In this research, we first presumed that a person who processes more emails would become careless and will tend to open the attachment, but here, we found the opposite pattern.

Note that no correlation with Attachment Opening on the 2nd delivery is observed. So we could say that even groups with less emails processed, can learn from training and education by inoculation.

Fig. 4-13) Average Number of Processed Emails per Day (Weekday) and Attachment Opening Status at 1st Delivery



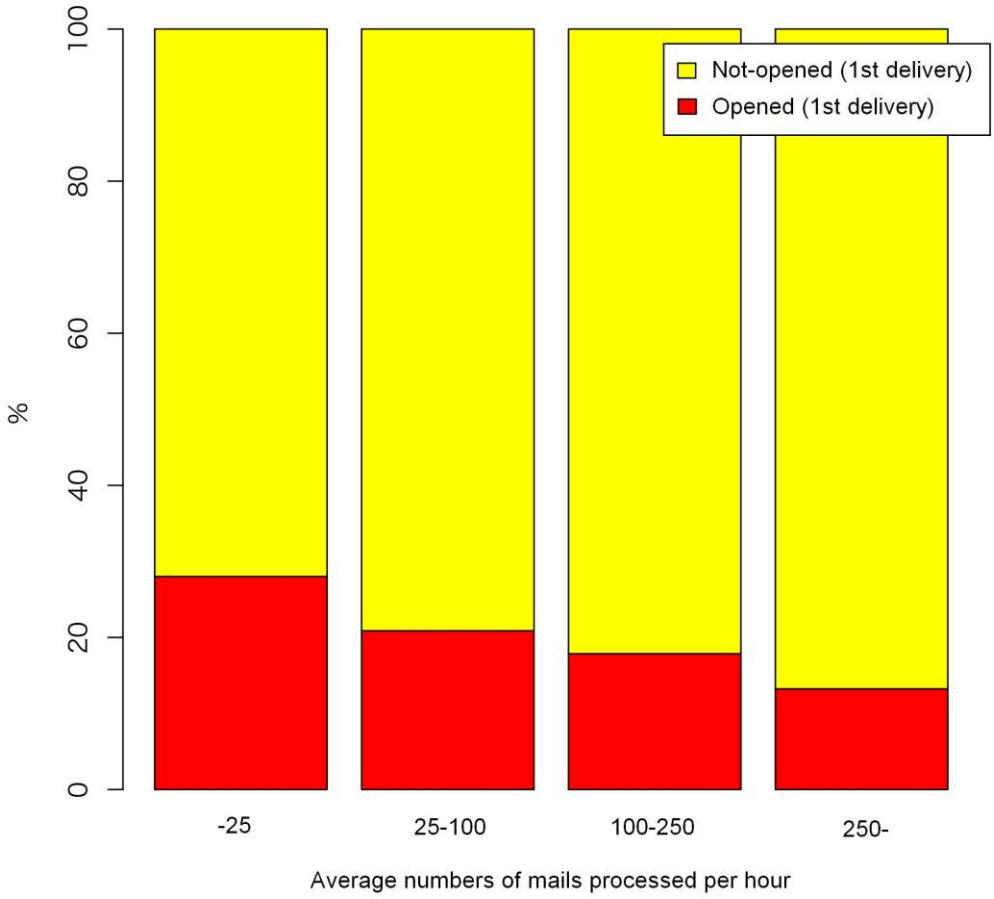
With regard to the Average Numbers of Emails Processed per Hour, the group with less numbers seems to have a high ratio of Attachment Opening, and the group with more numbers seems to have a low ratio of Attachment Opening.

With this attribute also, no correlation with the ratio of Attachment Opening on the 2nd delivery is observed. So we could say that Inoculation has a learning effect.

When considering all the patterns where the above Email proficiency “Poor” group is at risk, the groups with smaller Average Number of Mails Processed per Day is at risk, and the groups with smaller Average Number of Mails Processed

per Hour is at risk, email beginners who do not need to process so many emails have less chance to learn how to deal with emails, or be familiar with using emails.

Fig. 4-14) Average Number of Mails Processed per Hour and Attachment Opening Status at 1st Delivery



With regard to whether with or without experience of Inoculation, the Experienced group seems to have a lower Ratio of Attachment Opening, and the Not-experienced (this is the first time) group seems to have a higher Ratio of Attachment Opening.

There is nothing surprising as groups which have experienced the Inoculation

are provided with much more education / training, but it is one of the good reasons that Inoculation is effective.

Fig. 4-15) Inoculation Experience and Attachment Opening Status at 1st Delivery

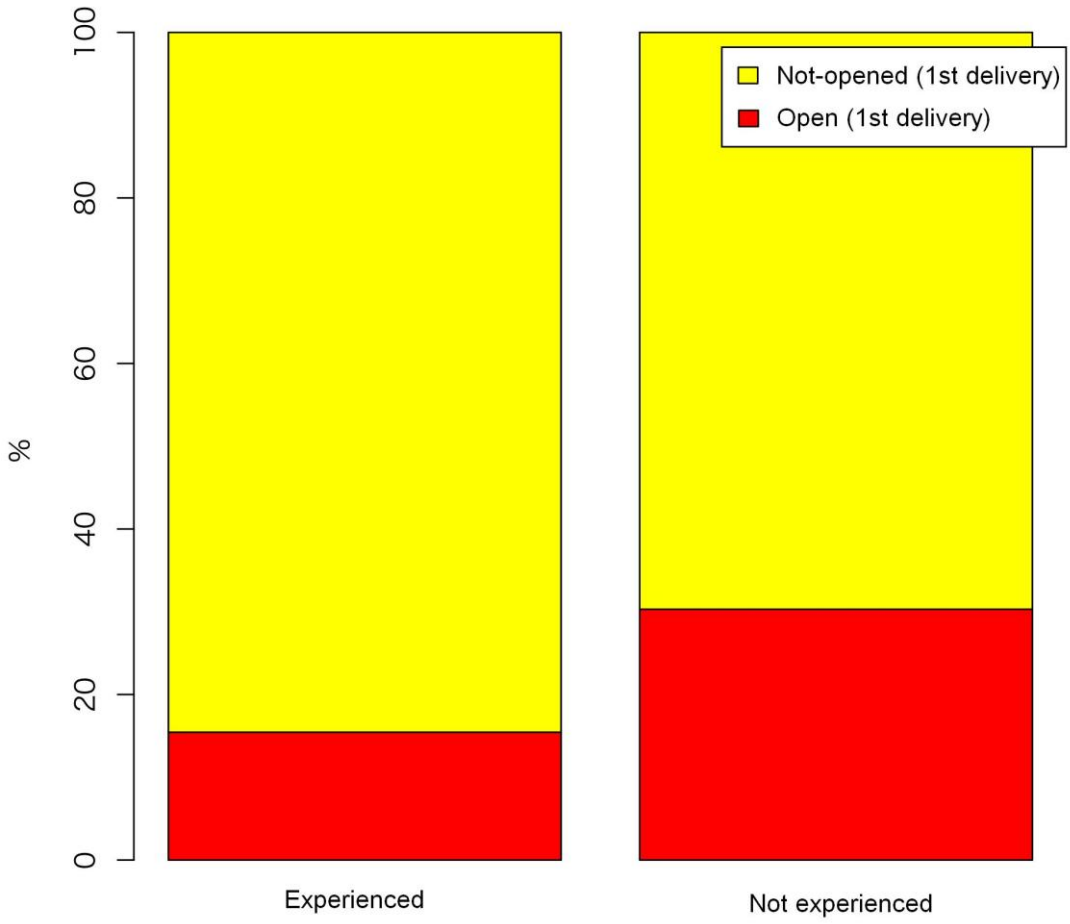
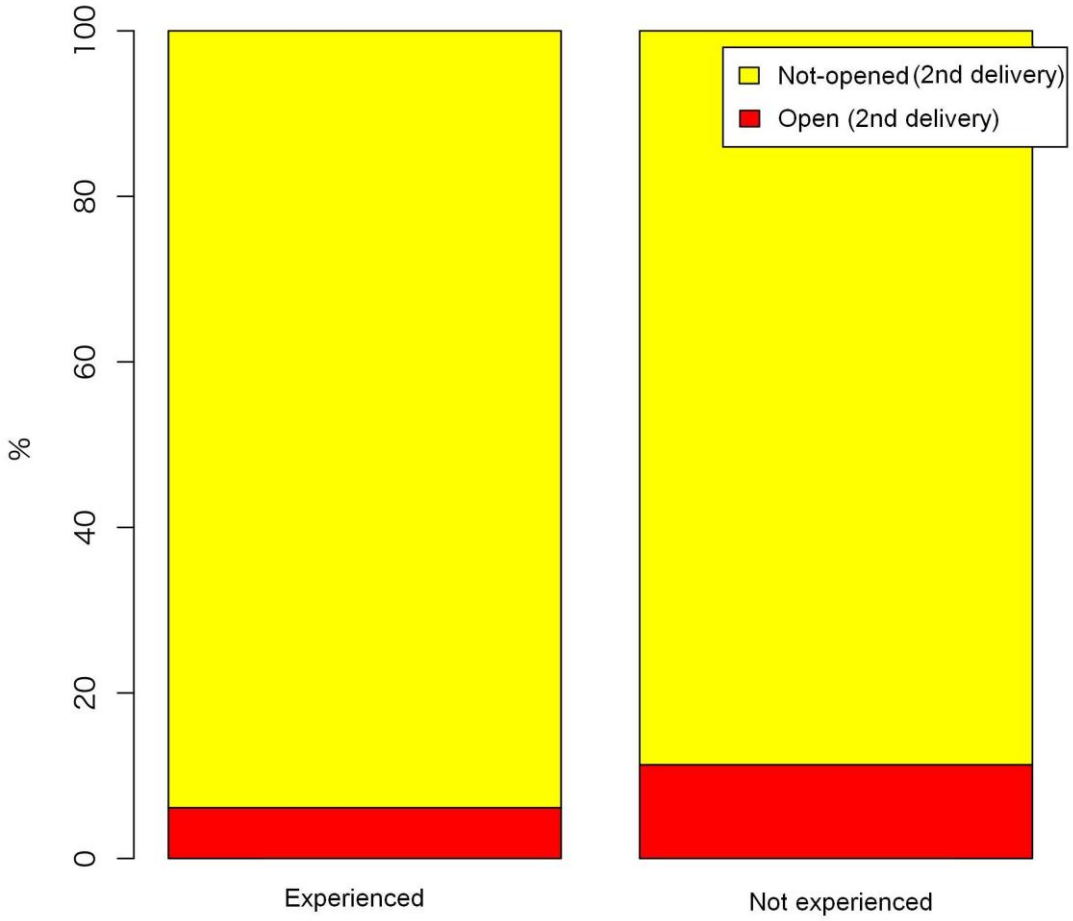


Fig. 4-16) Inoculation Experience and Attachment Opening Status at 2nd Delivery



It is hard to understand the correlation relating to Relevancy to Work.

It seems clear that if the group differs, there is significant difference statistically in the Ratio of Attachment Opened. Test result suggested that the groups which answered as “Very much related” and the groups which answered as “Not related” have high ratio of Attachment Opening, followed by “Much related” groups, and “Slightly related” groups have the lowest Ratio of Attachment Opening.

With regard to the correlation between Relevancy to Work and the Ratio of Attachment Opening, we should consider the correlation with the types of pseudo-attack mails, but it seems like that there is not sufficient data in this research. This should be discussed as a future issue.

Fig. 4-17) Relevancy to Work and Attachment Opening Status at 1st Delivery

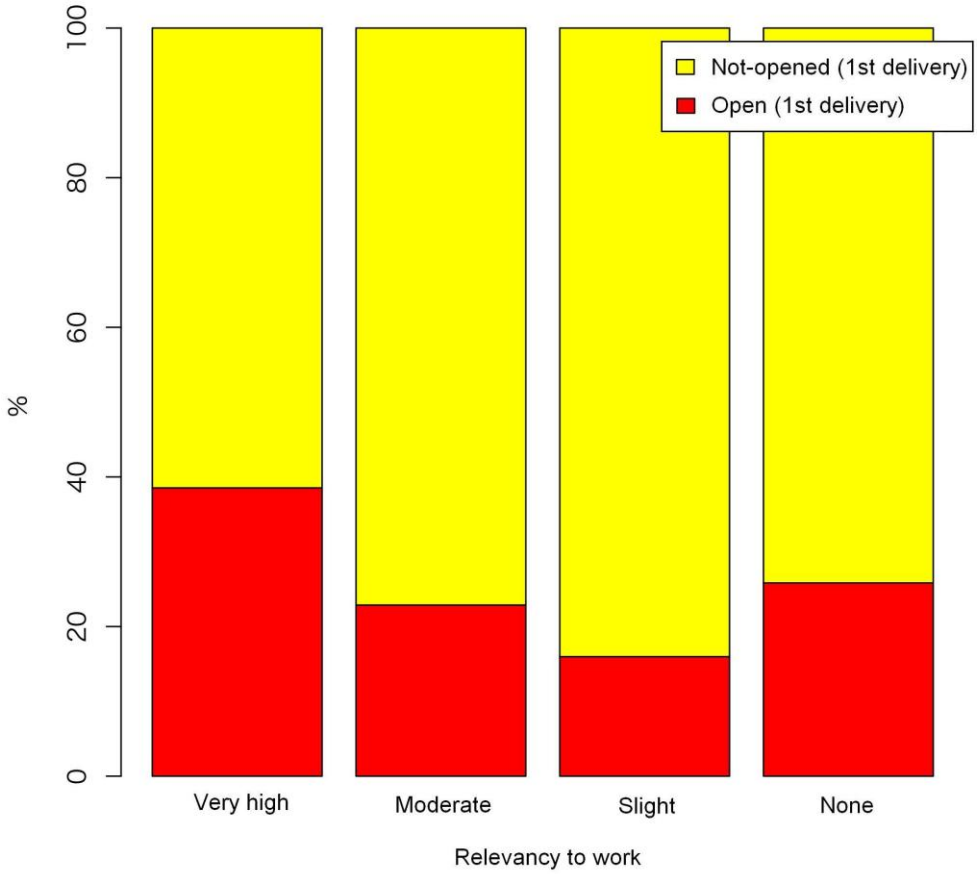
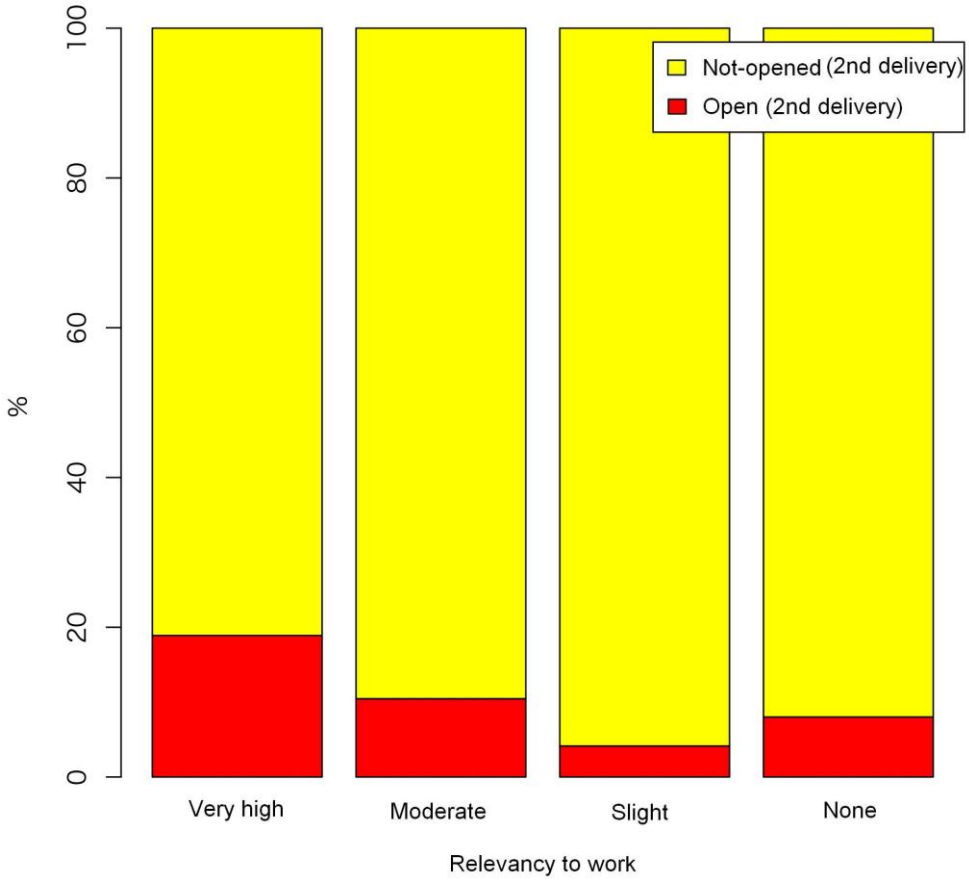


Fig. 4-18) Relevancy to Work and Attachment Opening Status at 2nd Delivery



4.5 Opinions and Comments

We received various answers for the Opinions and Comments area of the questionnaires. We have not counted these but there are common answers as follows.

1. Opinions and comments which show candid surprise and understandings toward the tactics of targeted email attacks through the experience of Inoculation.
2. Opinions and comments which say that we should perform trainings

regularly or repeatedly, sometime after.

3. Opinions and comments which say that if we perform trainings using Inoculation, we should use more sophisticated pseudo-attack mails

4. Opinions and comments which say that we should stop the Inoculation as they hinder the business operation.

5. Opinions and comments which say that we should stop inflow of spam into Participants' inbox by reinforcing spam countermeasures in an organization, as emails of targeted email attack are actually spam.

In pointing out an issue related only to the method of this research, this research is intended for user groups who do not have much technical knowledge or experiences to learn through experience. So we have no disagreement that skilled users who have opinions such as the one expressed in 3 above would feel somewhat disappointed with the training. However, considering that even this level of pseudo-attack email shows considerable Ratio of Attachment Opening, we would appreciate it if understanding that the current Inoculation Program approach is intended to increase the overall level.

As for opinion 4, we are awfully sorry but thinking of the significance of damages in the event of malware inflow, it is necessary to take measures against targeted email attacks. On the other hand, we need to make efforts to reduce the influence on business operations by performing preliminary training before the Inoculation or Follow-ups sufficiently.

As for the opinion 5, presumably each Subject Organization is taking measures against spam. However it is very difficult to eradicate targeted attack emails which get past the countermeasures. As such, we would appreciate if understand could be gained that we have no choice but to perform this kind of training.

5 Summary

The findings in this research are as follows:

1. In this research, the Ratio of Attachment Opening of the 2nd delivery, which was performed two weeks after the 1st delivery, has significantly decreased statistically compared to the 1st delivery. That is, Inoculation Program method has a learning effect.

2. As for the lifecycles of Improvement Rate, at the early stage in which we start the education/trainings related to targeted mail attacks, the Improvement Rate remains moderate. As education/trainings proceed, the Improvement Rate reaches its maximum, and then it would decline as education/trainings become widespread.

   Comparing the values of the Improvement Rate (2008 and 2009), 2009's Improvement Rate has significantly declined statistically.

3. As for the lifecycles of Learning Effect, at the early stage of education/trainings, the rate would remain moderate, and then the rate would increase and remain at a high 80% and above.

   Comparing the values of the Rate of Learning Effect (2008 and 2009), they do not have significant differences, and the above patterns can be identified from the graphs.

4. Lifecycles of Non-File-Opener Rate would be moderate at early stage, then the rate would gradually increase and remain at a high level.
   Comparing the values of the Non-File-Opener Rate (2008 and 2009), 2009's Rate has significantly increased statistically.

5. When looking at the chronological trend of Attachment Opening Status from the point when pseudo-attack mails were delivered, we could observe the following relationship:

   *Ratio of Attachment Opening (%) = (200/3) * arctan (3 * elapsed time after*

delivery (min.)/100)

This suggests that, within 30 minutes after the delivery, half of all the Participants have opened the attachment.

6. Though we attempted to compare the “strength” of the pseudo-attack emails (6 types) used in this research, the numbers of samples were insufficient, and as such, we were not able to identify a pattern. This should be discussed as a future issue.

7. The research suggested that Participant properties such as gender, age group and duties do not have much correlation with Open / Not-opened status. You can say that this is the same pattern as the Inoculation Program of the last fiscal year (2008).

8. Participants who answered "Poor" in response to the question of Mail Proficiency tend to have high risk. However; Participants may have determined their own Mail Proficiency based on the fact that they have opened the attachment file of the pseudo-attack mail.

9. Participants who have less Number of Mails Processed per Day tend to have high risk. This is the very opposite result from our initial hypothesis in this research.

10. Participants who have less Number of Mails Processed per Hour tend to have high risk. Also, this is the very opposite result from our initial hypothesis.

11. Considering the three points above, those who are email beginners and do not need to process so much mails have less chance to learn how to deal with emails, or be familiar with using emails, and therefore may be in the risk group, which is wide-open to targeted Email attacks.. As a catch-phrase, you can say “permanent mail beginners are at risk”

12. With or without experience of Inoculation shows a statistically significant difference in Ratio of Attachment Opening. That is, Inoculation Program is effective.

13. If the Relevancy to Work differs, there is a statistically significant difference in the Ratio of Attachment Opening. And it tends to have a high risk if the ratio shows “Very much related” or “Not related”.

In view of the objective of this research made at the beginning, you can say that the effect of acquiring resistance against targeted email attack through Inoculation Program methods has been verified statistically by comparing between the 1st and 2nd pseudo-attack email delivery of this year, or by comparing between last year and this year. Furthermore, as for the risk group hypothesis of this year, we can say that we were able to extract the risk groups, although the results were opposite with regard to our hypothesis.

As our future issues, verification of difference of “strength” between the 6 types of pseudo-attack mails, and verification of relationships between Relevancy to Work and the Ratio of Attachment Opening are remaining. We would proceed with further verification on our next occasion.