Security Measures Based on Human Behavior Characteristics

● Takeaki Terada ● Yoshinori Katayama ● Satoru Torii ● Hiroshi Tsuda

Recently, the number of targeted attacks has been rapidly increasing. Attackers limit their target to specific organizations or users and send targeted e-mails that cannot be easily identified as being malicious and steal data. In addition, large-scale information leakage accidents have occurred due to human errors such as missending of e-mail, and internal fraud. As a measure against missending of e-mail, Fujitsu has developed a tool that warns its users about making a mistake with regards to the recipients or attachments at the time of sending. To deal with targeted e-mails, we have extended the tool to alert users to suspicious incoming e-mails based on detection of differences with the header information of e-mails they have received before. Furthermore, we have also developed a technology to detect behavioral characteristics of individuals who are vulnerable to cyber-attacks by examining psychological characteristics and PC operation behavior of people who have experienced virus infection, fraud, or information leakage. These technologies will enable flexible security management based on the risk characteristics of individuals and organizations. This paper presents our technologies for reducing users' security risks, such as user interfaces that warn of e-mail missending and issue alerts for suspicious incoming e-mails, and risk assessment technology based on analysis of psychological characteristics and PC operation behavior of users.

1. Introduction

The majority of information leakage incidents within organizations are due to human error, and the management of people in the area of security is becoming an increasingly important issue. For example, according to a survey conducted by IBM, 47% of all information leakages are due to internal fraud or malicious attacks, 25% are due to human error, and 29% are due to system vulnerabilities.[1)]

Information leakage incidents due to fraud within organizations continue to occur, and those who intentionally leak database are subject to be punished under the latest revision of Japan's Act on the Protection of Personal Information (provisional translation). Moreover, typical incidents of human error such as missending of e-mails still make newspaper headlines.

Targeted attacks, a type of malicious attack from the outside that has become a hot topic in recent years, target people with low security awareness after penetrating systems by using reconnaissance through social engineering or clever targeted e-mails. Targeted e-mails cleverly impersonate customers or relevant parties, making them difficult to recognize as threats for general users. Therefore, efforts to raise the level of security awareness against targeted attacks through training or education are important.

This paper introduces measures based on an alert-type interface and initiatives in the area of technologies for the analysis of psychological and behavioral characteristics and reduction of security risks due to human error.

2. Tool to prevent e-mail missending

Missending of e-mails is a typical human error and even now commonly occurs owing to erroneous CCing and BCCing or other such mix-ups. The causes of missent e-mails are numerous. The authors analyzed such instances within their own organization and found that in the majority of cases, the cause is erroneous selection of the receiver's address or file mix-ups. Based on this finding, the authors then developed a tool that issues alerts in real time when users attempt to send

e-mails that match e-mail patterns particularly susceptible to mistakes (**Figure 1**).

Analysis of the usage log of this tool, covering a total of about 14,000 e-mails revealed a recovery rate (percentage of e-mail transmissions stopped as the result of an alert issued by this tool: Potential missending probability) of approximately 1%. This exceeded the initially anticipated missending rate. According to interviews with persons who recovered e-mails, there were many cases where that extra step required for sending e-mails made them realize errors, even if not necessarily missending errors, such as, for example, having forgotten to include needed information in the body of the e-mail. Further, the data revealed that the average missending rate rises to close to 2% between 1 p.m. and 3 p.m., indicating that this is a time period when concentration drops. Thus, it was demonstrated that use of this tool is effective to prevent missending.

On the other hand, a shortcoming of alert-type tools is that repeated output of alerts gradually causes habituation in users. In this regard, this tool, based on the human memory model (forgetting curve), is designed to learn automatically high-frequently destinations from the outgoing e-mail history and eliminates the need to frequently perform the same checks. This tool is currently being sold as the "FUJITSU Security Solution SHieldMailChecker E-mail Missending Prevention" by Fujitsu Social Science Laboratory.[2] About a hundred thousand Fujitsu employees use this as a standard tool.

3. Targeted e-mail threat protection tool

Targeted e-mails in many cases impersonate customers or relevant parties, making them difficult to recognize as threats for general users. Furthermore, malware of types not detectable by commonly used anti-virus software is used, making detection by file inspection tools difficult. In addition, new targeted e-mail techniques are being developed one after the other—including back-and-forth type attacks, which causes infection after multiple exchanges done by impersonating customers, and watering hole attacks that implant malware in websites frequently visited by the targeted person.

Improving users' ability to detect such suspicious e-mails and reducing the risk of targeted attacks can be said to be realistic approaches. For example, targeted e-mails that impersonate a sender in the "From"

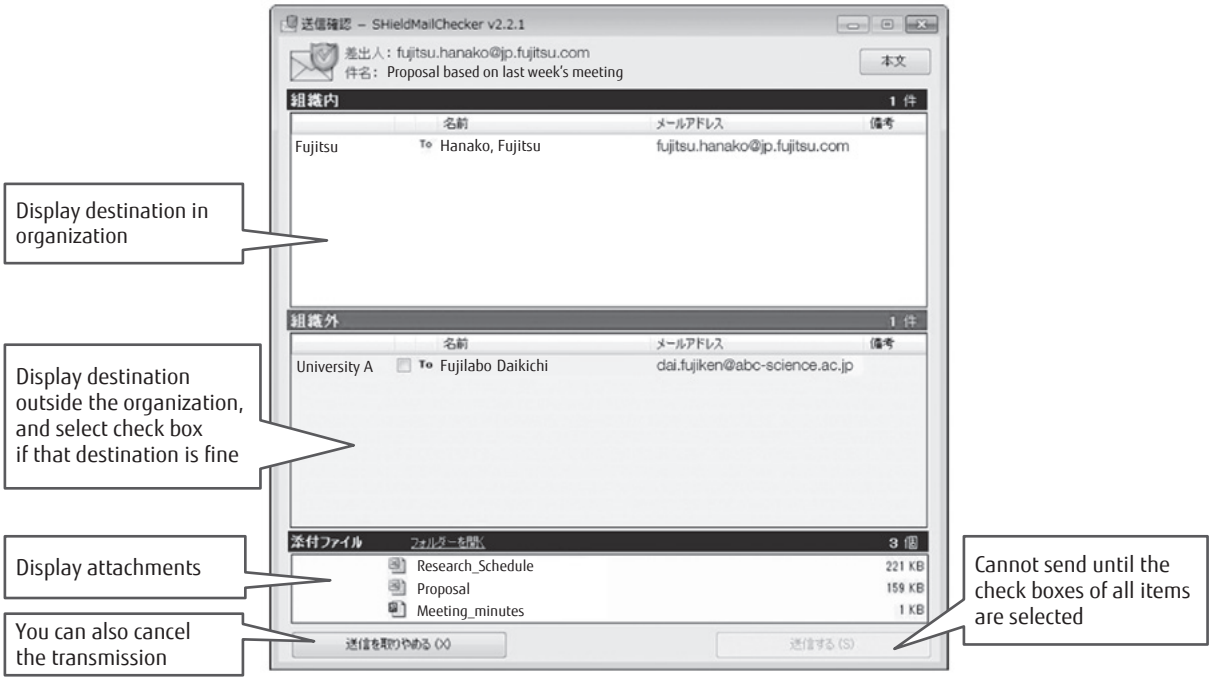

Figure 1
Tool to prevent e-mail missending.

field (sender's e-mail address) in the e-mail header are difficult to see through based solely on the content of the e-mail. However, by using the characteristics of the e-mail header, users can be made aware of the suspiciousness of an e-mail. Thus, the authors developed a tool that issues alerts in real time upon detecting spoofing e-mails by learning the feature values of Received, Reply-To and other elements of the e-mail header of past e-mails from the same person and comparing them with the header of the newly incoming e-mail (**Figure 2**).[3)]

In a test in which targeted e-mails were sent to 20 users of this tool and 33 non-users, only one user of this tool opened the e-mail, compared with 11 non-users. Thus even for targeted e-mails, this tool is considered to have a certain level of alert effectiveness. This tool has been also launched as the "FUJITSU Security Solution SHieldMailChecker Spearphishing E-mail Protection" by Fujitsu Social Science Laboratory.

4. Psychological characteristics of persons who have experienced cyber attacks

Virus infections caused by targeted e-mails or access to malicious websites, and money losses and account compromise caused by phishing e-mails and the like are regarded as being attributable in part to users. Failure to fully implement security measures established by the ICT administration department because of too much work, failure to notice suspicious aspects of received e-mails or web pages when in a rush to complete work, and overconfidence in one's ability to use personal computers and the Internet are considered to be contributing psychological states. To make the alert-type user interface described in the previous section even more effective, it is necessary to analyze why people become victims of information leakages and cyber fraud in the first place. Particularly in the case of information leakages where customer information or confidential information gets leaked through the likes of e-mails and social networking services (SNSs), the causes on the user side ought to be investigated thoroughly.

According to research in the field of social psychology, human perception of risks in the real world, such as disasters and infectious diseases, vary depending on the psychological state of the person, as described above. The following presents some of the findings of psychology regarding human perception of risk.

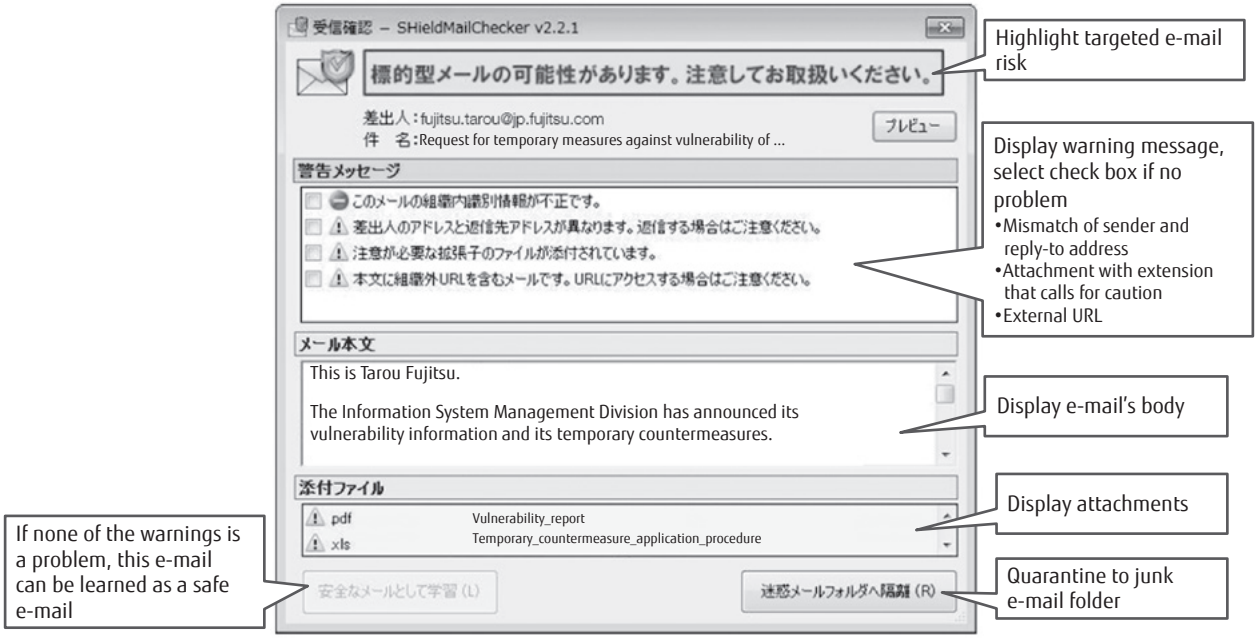

Figure 2
Targeted e-mail threat protection tool.

1) Cost perception

Indicates the level of psychological burden felt where there are measures to reduce risk. Persons who have a low level of cost perception are more likely to go ahead with the implementation of information security measures without making a fuss.

2) Benefit perception

This indicates the degree to which priority is placed on merits rather than risk. Persons who have a high level of benefit perception are more likely to be interested in the content of an e-mail if it looks suspicious, and suffer damage.

3) Controllability

This indicates the degree to which one perceives that one can control risk oneself. When this perception is too acute, the psychological state of the person can be said to be one of overconfidence, and such a person is more likely to engage in careless behavior on PCs and the Internet.

4) Status quo bias

This indicates the psychological tendency to favor habits when it comes to action. Persons with a strong status quo bias are more likely to click as usual to open an e-mail or website URL even if they feel that it is a little suspicious, and thus to be vulnerable to attacks.

In reference to the traditional knowledge above, the authors conducted a survey examining the characteristic psychology of about 2,000 persons who experienced firsthand within the past two years a computer virus infection, cyber fraud, or information leakage.[4] The subjects were Internet users in Japan who use personal computers for the majority of their work.

Table 1 lists the main psychological characteristics observed in persons who have made any of the above three experiences. The results of the analysis revealed that many users with strong benefit perception have experienced virus infection or cyber fraud, and that many users who are overly confident in their operation of personal computers have experienced information leakage. Measures to mitigate such tendencies, for example informing users about instances of people they know who have experienced such things, are believed to raise the risk awareness of these users and reduce the number of such incidents.

5. Risk assessment tool based on PC operation logs

In order to proactively use psychological characteristics described in the previous section to protect users on a daily basis in enterprises, the Security Department needs to conduct surveys frequently to quickly verify changes in the danger level of the psychological characteristics of employees. However, this imposes a great burden on both employees and the security department. Further, the degree to which psychological characteristics are manifested tends to vary greatly depending on the circumstances. For example, if one receives urgent work, has a large amount of work, or starts feeling unwell, one's psychological characteristics are likely to change, and even a low-risk person may become more at risk of experiencing mishaps when exposed to increased mental stress. In view of the above, the authors have been developing technology to detect users at high risk by determining their risk of suffering damage, by assessing their psychological characteristics through analysis of PC operation logs, based on an examination of the relationships between

Table 1
Psychological characteristics of persons who have experienced cyber attacks.

Characteristic	Explanation of characteristic	Virus	Information leakage	Fraud
Heavy psychological burden	Security measures are very cumbersome		✓	✓
High benefit perception	Tendency to emphasize advantages even when risk is slightly high (for example, crossing a road at a red light)	✓		✓
Strong status quo bias	Tendency to favor habits when it comes to action (for example, continuing to watch TV or surf the Internet)		✓	
Overconfident	Overconfidence in one's PC skills		✓	
Low information sharing intent	When makes a mistake in the course of business, tries to fix it him/herself without consulting those around		✓	
Strong cost perception	Reluctant to make strong efforts to reduce risk	✓		

psychological characteristics and PC operation logs.[5)]

First, to examine the relationship between psychological characteristics and PC keyboard and mouse operation logs, the authors surveyed 30 developers and tabulated PC operation log data. Based on the trends obtained as the result of this analysis, the authors then created an experimental demonstration tool for assessing the potential risk of users. We elected to create an application to be installed on PCs and made 221 employees spread across multiple departments try it out. Besides getting the participants to answer a ten-question survey titled "Assess Your IT Risk," we recorded the operation log while the participants were taking the survey. Permission for log acquisition was obtained beforehand from the participants through the Terms and Conditions the survey. The survey answers revealed the following two major findings.

1) Keyboard and mouse operation while the Terms and Conditions were displayed on the screen

One of the behavioral characteristics of PC operation was investigated by observing whether the participants duly read the Terms and Conditions displayed when installing applications and software. For that purpose, a Terms and Conditions screen was displayed prior to the start of the actual survey. Log recording began from the time this screen first appeared, but the log was discarded if a participant closed the Terms and Conditions screen without first clicking the [I agree to the above] button. Upon conclusion of the survey, the mouse cursor paths, heat map, and display durations of the Terms and Conditions were displayed. The heat map divides the Terms and Conditions screen into a grid, and totals the number of times the mouse cursor of each participating user has passed over each grid cell, presenting that frequency with different colors (**Figure 3**). The dark box in the upper left in the figure represents the color red as displayed on the actual screen, and the closer to the color red a grid cell is, the more times users passed their mouse cursor over that grid cell. The results of the analysis reveal that those persons who carefully checked the Terms and Conditions tended to move their mouse cursor to various places over the screen and the screen display time tended to be long, whereas persons who did not check the screen for a long time tended to display the screen for a short time only, moving their mouse cursor in a straight line to the survey start button in the lower right of the screen.

2) Risk assessment results

Figure 4 shows the values of damage risk (not

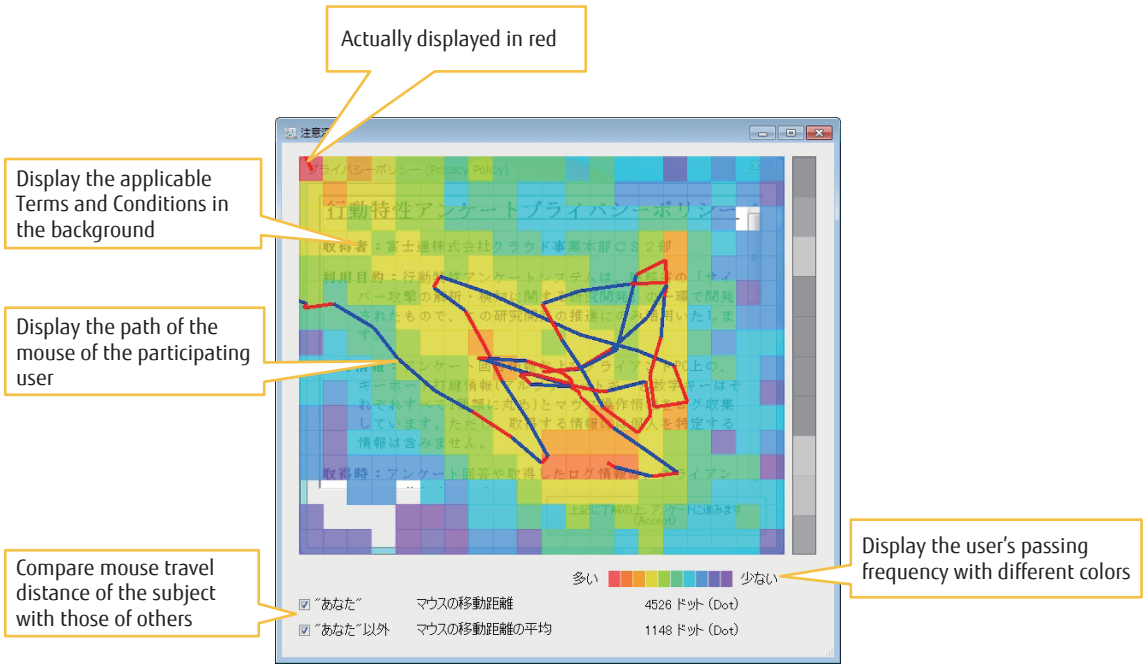

Figure 3
Mouse path on Terms and Conditions screen.

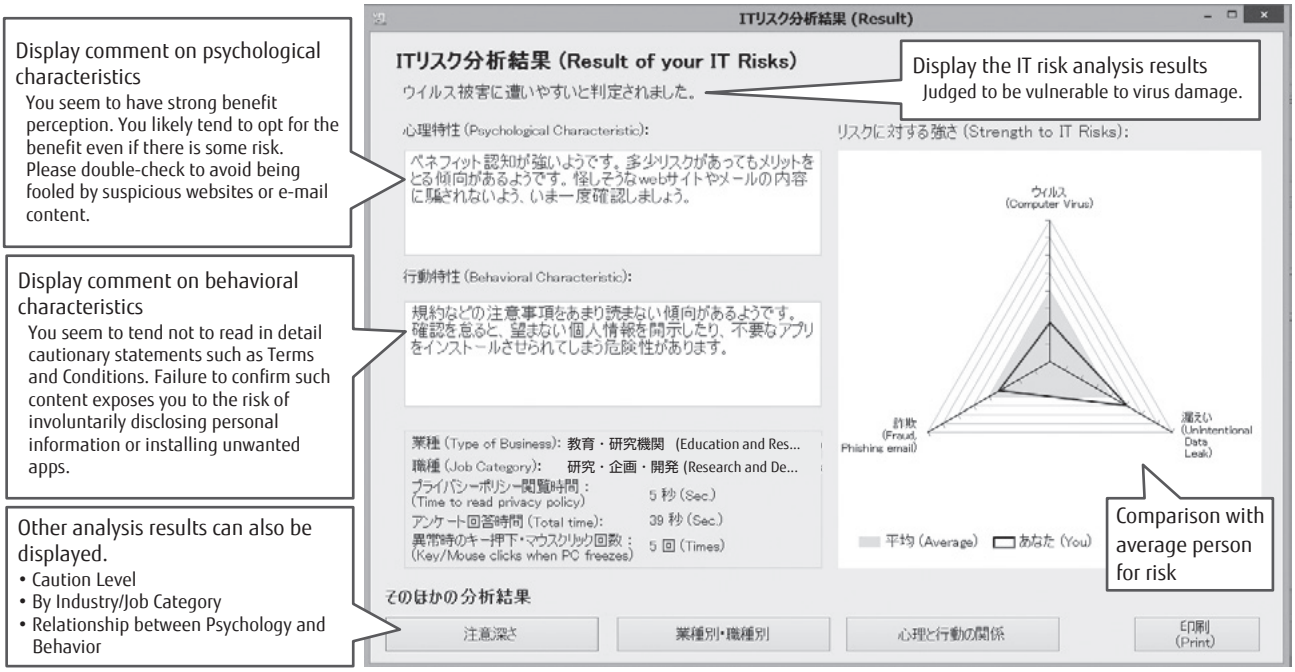

Figure 4
Risk assessment screen.

displayed in this journal), as obtained from the acquired survey responses and from the operation log, along with the average value for all users, in the form of a radar chart, for the three types of damage, i.e. computer virus infection, cyber fraud, and information leakage. A comparison of the averaged damage risk values by industry and job category reveals differences.

Table 2 lists the results of the analysis of the relationship between the survey responses of 221 persons and the operation log taken during survey taking. Persons with high benefit perception and cost perception tended to display the Terms and Conditions screen for a short time only, whereas risk-averse persons tended to make few key presses when the PC froze. PC freezes as described here were produced by not responding to key inputs for a certain number of seconds during survey taking with the tool developed by the authors. Compared with other generations (20s, 40s, and over), persons in their 30s showed a tendency to not read the Terms and Conditions carefully, and persons holding executive positions tended to make fewer key presses when the PC froze.

Table 2
Relationship between psychological characteristics and behavioral characteristics of persons who have experienced cyber attacks.

		PC behavior characteristics
Psychological characteristics	Strong benefit perception	Short display duration of Terms and Conditions
	Prefers to avoid risk	Small number of key presses when PC freezes
	Low cost perception	Long display duration of Terms and Conditions
Other characteristics	Age: 30s	Short display duration of Terms and Conditions
	Executive position, age other than 20s	Small number of key presses when PC freezes

6. Conclusion

This paper introduces an initiative by Fujitsu to reduce the frequency of information security accidents caused by human error and clever targeted attacks. Technology using an alert-displaying application to prevent missending of e-mails and becoming the victim of targeted e-mails was put to practical use at Fujitsu, showed a certain degree of efficacy, and thus was commercialized.

To further strengthen the technology, the authors conducted further surveys of the psychological characteristics of persons who experienced any of the three

types of damage of computer virus infection, cyber fraud, and information leakage. As a result, persons with strong benefit perception and overconfident persons were found to be more likely to experience damage. Moreover, in applying technology for automatically detecting user at high risk of damage by assessing psychological characteristics through analysis of PC operation logs, a correlation was found between a high level of benefit perception and cost perception and shortness of the time spent reading the Terms and Conditions. Going forward, we believe that advance detection of users and departments at high risk will become possible without imposing a burden on users and administrative departments through the establishment of technology to analyze the psychological characteristics of persons who have suffered damage and technology to assess damage risk based on PC behavior characteristics.

Part of this study has been conducted under "Research and Development for the Analysis and Detection of Cyber Attacks" commissioned by the Ministry of Internal Affairs and Communications of Japan.

References

1) IBM, Cost of Data Breach Study, 2015.
2) T. Takebayashi et al.: Data Loss Prevention Technologies. FUJITSU Sci. Tech. J., Vol. 46, No. 1, pp. 47–55 (2010). *http://www.fujitsu.com/global/documents/about/resources/publications/fstj/archives/vol46-1/paper13.pdf*
3) T. Yoshioka et al.: A Client-side Solution for Protection against Targeted Email Attacks Using Email Feature Information. IPSJ Journal, Vol. 55, No. 10, pp. 2290–2299, Oct. 2014 (in Japanese).
4) T. Terada et al.: Investigation on Psychological and Behavioral Characteristics of Users Vulnerable to Cyber Attack. Proceedings of Multimedia, Distributed, Cooperative, and Mobile Symposium (DICOMO2014), pp. 1498–1505, IPSJ, 2014 (in Japanese).
5) Y. Katayama et al.: An Attempt to Visualization of Psychological and Behavioral Characteristics of Users Vulnerable to Cyber Attack. The 32nd Symposium on Cryptography and Information Security (SCIS2015), 4D1-3, IEICE, 2015 (in Japanese).

Takeaki Terada
Fujitsu Laboratories Ltd.
Dr. Terada is currently engaged in cyber security related research and development.

Yoshinori Katayama
Fujitsu Laboratories Ltd.
Mr. Katayama is currently engaged in cyber security related research and development.

Satoru Torii
Fujitsu Laboratories Ltd.
Mr. Torii is currently engaged in cyber security related research and development.

Hiroshi Tsuda
Fujitsu Laboratories Ltd.
Dr. Tsuda is currently engaged in research and development of information leakage countermeasures.