International Journal of Networking and Computing – www.ijnc.org, ISSN 2185-2847
Volume 11, Number 2, pages 412–425, July 2021

Information Security Fatigue Countermeasures Using Cognitive Strategy Scale Based on Web Questionnaires

Misato Ogawa
Faculty of Social System Science
Chiba Institute of Technology
Narashino, Japan
g1642028.cit@gmail.com

Shigeaki Tanimoto
Faculty of Social System Science
Chiba Institute of Technology
Narashino, Japan
shigeaki.tanimoto@it-chiba.ac.jp

Takashi Hatashima
NTT Secure Platform Laboratories
Nippon Telegraph and Telephone Corporation
Musashino, Japan
takashi.hatashima.ch@hco.ntt.co.jp

Atsushi Kanai
Faculty of Science and Engineering
Hosei University
Koganei, Japan
yoikana@hosei.ac.jp

Received: February 5, 2021
Revised: April 28, 2021
Accepted: June 14, 2021
Communicated by Yasuyuki Nogami

Abstract

Information security measures have become increasingly important not only for companies but also for individuals in recent years. For this reason, many information security measures have been taken. However, if information security is overly complicated, ICT users may get overwhelmed. Although research on information security fatigue is being conducted, currently it is not enough. In particular, research from a psychological point of view is lacking. Examples of psychological measures include cognitive strategies that are classified as behavioral models. There are various cognitive strategies, but research into particular countermeasures against information security fatigue has not been sufficiently explored. In this work, we propose new measures based on psychological viewpoints. Specifically, these are information security fatigue countermeasures that introduce a cognitive strategy. We conducted a questionnaire survey on cognitive strategies and information security fatigue, analyzed the results, and classified them into 24 levels, consisting of six levels of the information security fatigue scale multiplied by four levels of cognitive strategies. Then, for each of these 24 levels, a new information security fatigue measure was proposed and evaluated on the basis of the free responses of the questionnaire survey. The results indicated that appropriate information security fatigue countermeasures according to human behavior patterns based on cognitive strategies and the information security fatigue scale are possible.

Keywords: Cognitive Strategy, Information Security Fatigue, Security Policy, Security Countermeasures

1 Introduction

In recent years, the number of security incidents has been increasing along with the rapid development of the Internet [10], and information security measures are important not only for companies but also for individuals. The main information security measures include the introduction of antivirus software, OS updates, use of multi-factor authentication, and alerts to suspicious sites and email attachments.

In general, information security measures tend to become more stringent and complex with the occurrence of security incidents. Since severe and complex information security policies may cause "security fatigue" and "security burnout", which is the deterioration of the information security condition, Hatashima et al. [5]–[7] introduced the information security condition matrix to help combat this. However, their studies were limited to visualizing the information security fatigue scale and did not sufficiently consider concrete countermeasures, especially psychological measures.

The cognitive strategies that classify human behavioral patterns [11] are one example of psychological countermeasures. Cognitive strategies include consistent patterns of expectation, evaluation, planning, effort, and retrospection as individuals pursue personally relevant goals. There are various taxonomies of cognitive strategies. For example, Mitsunami [11] explained that "Norem & Cantor categorized four cognitive strategies according to their perceptions of past performance and expectations of future performance". However, the application of this cognitive strategy to information security fatigue has not been fully explored.

In this paper, we propose a cognitive strategy that has four cognitive patterns (Low Metacognition etc.) [17] as a countermeasure for the psychological aspect of information security fatigue [5]–[7], based on the above background and from the psychological perspective. This makes it possible to take countermeasures based on 24 levels of states by multiplying the six levels of the information security fatigue scale of the previous study by four levels of cognitive strategies. Thus, in our contribution, detailed countermeasures against information security fatigue can be taken, which is expected to reduce security incidents such as information leakage due to internal fraud.

In Section 2 of this paper, we describe the current status and issues of information security fatigue. Section 3 describes our questionnaire survey to propose a new information security fatigue measure based on cognitive strategies. In Section 4, based on the results of the questionnaire survey, we clarify that the cognitive strategy can be applied. Furthermore, based on the open-ended responses regarding information security measures in the questionnaire survey, we newly propose information security fatigue countermeasures for each of the 24 levels by multiplying four levels of cognitive strategies by six levels of the information security fatigue scale. We conclude in Section 5 with a brief summary and mention of future work.

2 Current status and issues with information security fatigue

2.1 Current state of information security fatigue

2.1.1 Vicious cycle due to strict security operations

With the increase of cyber-crimes, information security is becoming more important, and various security policies to operate the security technology are being defined. However, if these procedures are too stringent, they may lead to a decrease in security awareness among employees, resulting in a disregard for security policies—for example, by using passwords inappropriately—which may lead to the eventual collapse of the security policy [8]. Generally, companies take information security measures to prevent information leakage incidents and accidents, but they tend to establish very strict rules at the initial stage. Employees typically recognize that the rules are necessary to protect security and they follow them, even if their operational efficiency is slightly reduced, but as time passes, the organization gradually falls into a vicious cycle in which the rules are no longer followed, as shown in Fig. 1 [16]. This situation in which the information security policy is not properly adhered to is one of the main reasons information security policies are not properly operated. As such, countermeasures against the vicious cycle created by strict rules is an important issue.

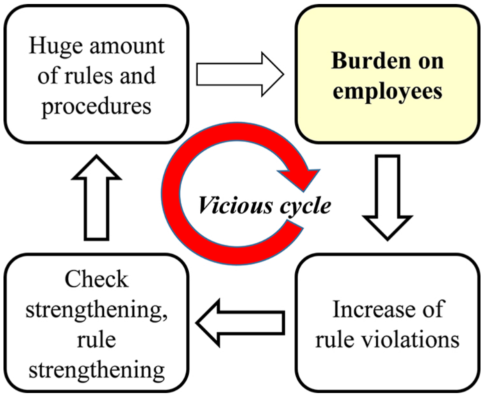

Huge amount of rules and procedures
Burden on employees
Vicious cycle
Increase of rule violations
Check strengthening, rule strengthening

Figure 1: Vicious cycle of strict rules.

2.1.2 Security fatigue proposal

The National Institute of Standards and Technology published a report on security-related stress [12] in which they examine a form of security-related stress called security fatigue, which is defined as "the fatigue produced by working on computer security measures". In addition, at SOUPS 2016 (Twelfth Symposium on Usable Privacy and Security), researchers such as Parkin et al. [15] discussed the security fatigue caused by security measures (e.g., two-factor authentication) that are required to be implemented as a routine task. The factors affecting this fatigue are explained by a cognitive control model, but these models are defined and proposed on the basis of individual cases, and there has not been enough systematic study on security fatigue as a whole.

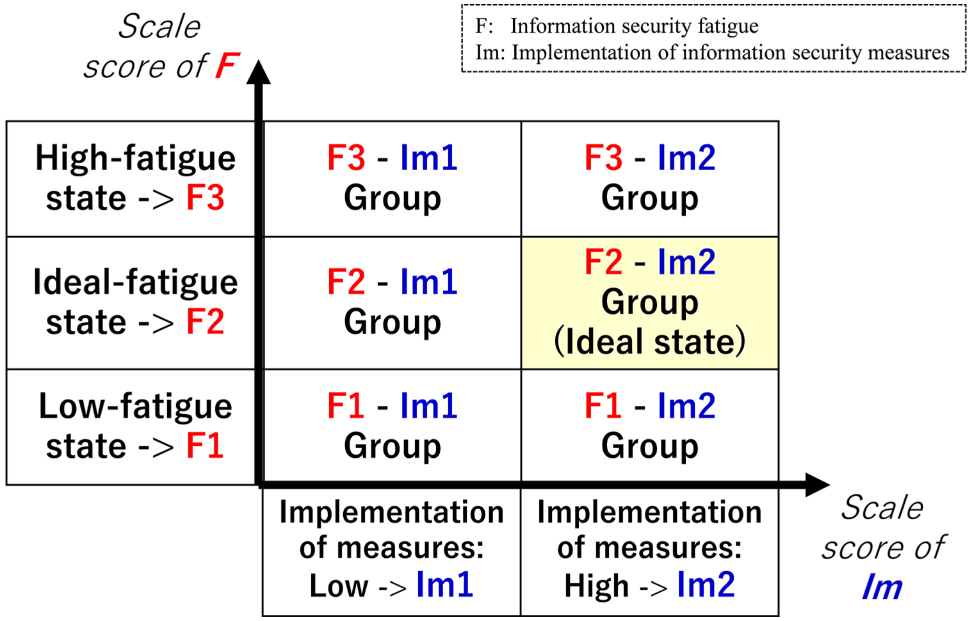
2.1.3 Information security condition matrix: Establishment of information security fatigue measurement scale

Hatashima et al. investigated the visualization of and solutions to information security fatigue and proposed an information security condition matrix based on the information security fatigue measurement scale as a means to visualize the state of information security fatigue [5]–[7].

Concretely, as shown in Fig. 2, the attitude of ICT users towards information security measures is expressed in a two-dimensional finite number of states by combining the newly established information security fatigue scale with multiple measurement scales based on the degree to which the security measures are implemented.

In Fig. 2, the results of latent rank theory analysis based on a questionnaire survey show that the ideal group is the F2-Im2 group, which had a high degree of security measure implementation (value on the horizontal axis: Im2) and a moderately strained state of information security fatigue (value on the vertical axis: F2) [3]–[4].

In other words, it is possible to determine the current state of information security fatigue by visualizing it in a two-dimensional matrix based on the information security fatigue measurement



F: Information security fatigue
Im: Implementation of information security measures

Scale score of F			
High-fatigue state -> F3	F3 - Im1 Group	F3 - Im2 Group	
Ideal-fatigue state -> F2	F2 - Im1 Group	F2 - Im2 Group (Ideal state)	
Low-fatigue state -> F1	F1 - Im1 Group	F1 - Im2 Group	
	Implementation of measures: Low -> Im1	Implementation of measures: High -> Im2	Scale score of Im

Figure 2: Information security condition matrix (cited in Ref. [6]).

scale and the degree of implementation of security measures, which makes it easier to manage the ideal security state (F2-Im2 group). Specifically, we can implement information security measures for each state of the information security condition matrix. It is also possible to detect information security fatigue at an early stage and prevent users from becoming exhausted with the information security measures by changing the measures flexibly and dynamically in response to the increasing or decreasing trends of the information security fatigue by monitoring the progress.

2.2 Issues of information security fatigue

As discussed above, we can take appropriate measures according to the state of fatigue by visualizing the information security fatigue. In other words, if we visualize the information security fatigue, we should be able to resolve the vicious cycle (Fig. 1) and prevent information security incidents such as internal fraud or information leakage. However, specific measures using the information security fatigue scale have not yet been fully explored, as we have only just begun to study them.

3 Proposal of information security fatigue measures based on cognitive strategies

In this paper, we propose a new information security fatigue countermeasure based on the classification of cognitive strategies using the Information Security Fatigue Scale. The proposed countermeasure is based on the results of our Web-based questionnaire analysis of working adults.

3.1 Cognitive strategies: Four patterns of classification

A cognitive strategy is “a consistent pattern of expectation, evaluation, planning, effort, and retrospection as an individual pursues a goal” [2]. Norem & Cantor classified cognitive strategies into four categories—strategic optimism (SO), defensive pessimism (DP), unjustified optimism (UO), and regular/realistic pessimism (RP)—according to perceptions of past performance and expectations of future performance, as shown in Fig. 3 [13].

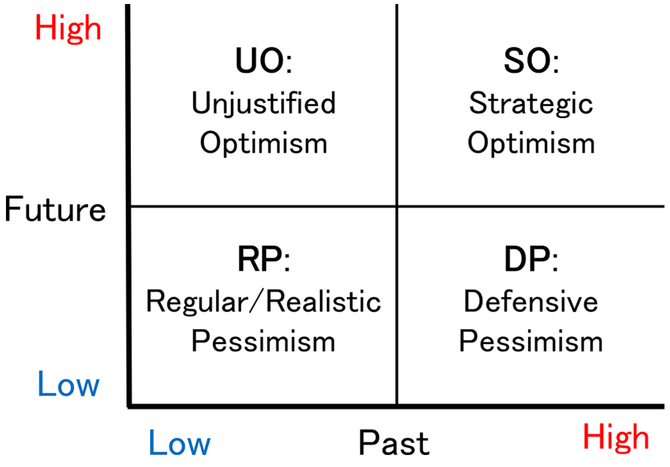


Figure 3: Classification model of cognitive strategies.

Table 1: Classification of cognitive strategies by Toyama [17].

Cognitive strategies	Features
Low Metacognition (LM)	Metacognition refers to the control of one's cognitive activities (perception, emotion, memory, thought, etc.) by objectively grasping and evaluating them. The LM group is defined as those with low metacognitive ability.
Regular/realistic Pessimism (RP)	The RP group is a group of people who think everything is negative and have a gloomy outlook on the future.
Defensive Pessimism (DP)	The DP group refers to people who strive to brighten their future by thinking about things in a negative way.
Regular/realistic Optimism (RO)	The RO group is a group of people who think everything is good and have a positive outlook on the future.

In contrast, Toyama developed a cognitive strategy that can identify deliberation as either "deliberation on the result" or "deliberation on the evaluation" [17] using the four patterns shown in Table 1. In this paper, we use Toyama's classification, which is more specific in terms of proposing security measures.

3.2 Web-based questionnaire survey to analyze cognitive strategies and information security fatigue

We conducted a Web-based questionnaire survey based on the cognitive strategy scale created by Toyama [17] and the information security fatigue scale created by Hatashima et al. [5]–[7]. In order to investigate security measures that combine the information security fatigue scale in Fig. 2 and the cognitive strategy scale in Table 1, we created each of the questions by citing the results of previous studies and conducted a Web-based questionnaire [14].

The Web-based questionnaire survey was conducted from December 23 to December 25, 2019. The survey was outsourced to a contractor [1]. At total of 521 working adults responded. We conducted a cluster analysis (Ward's method [9]) based on the standard scores of each subscale of the same cognitive strategy scale as Toyama's scale [17] on 459 respondents (excluding those who had provided dishonest responses; concretely, we included a question that could always be answered by reading the questionnaire, and excluded respondents who answered this question incorrectly).

As shown in Fig. 4, the standard scores for each scale in the four-cluster classification (anticipation and contemplation of failure, contemplation of success, contemplation of the plan, and recognition of past performance) yielded the same pattern, either high (+) or low (−), when the standard score was set to 0, as reported by Toyama [17].

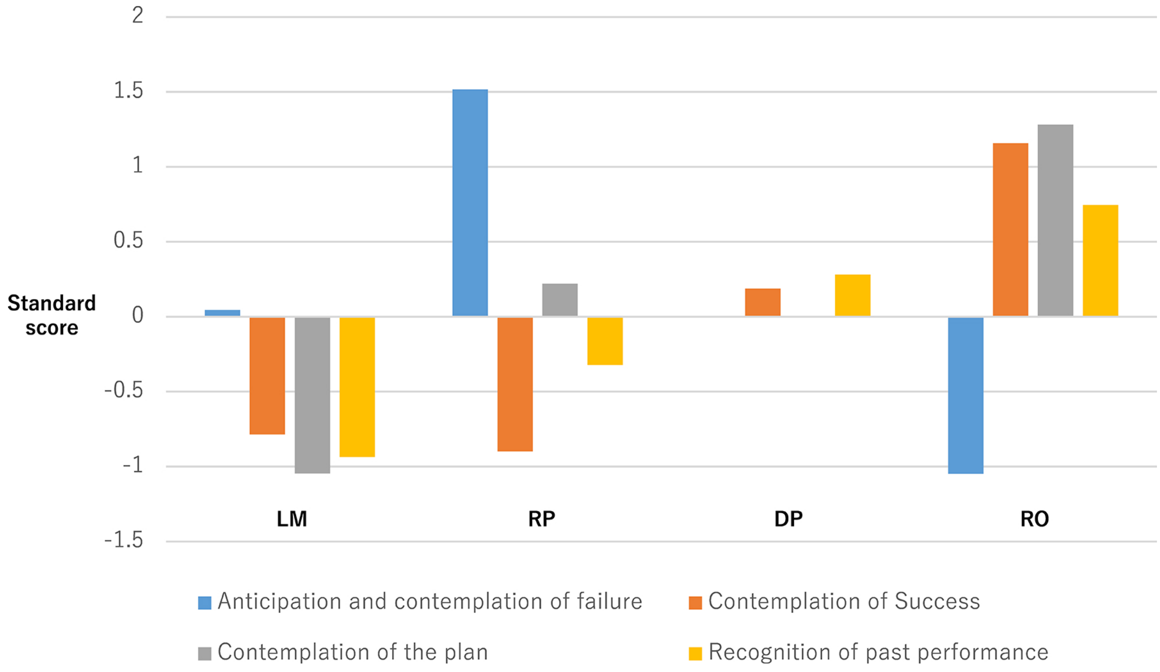


Figure 4: Results of cluster analysis (distribution of standard scores on the cognitive strategy scale by cluster).

Specifically, these are as follows. The numbers in parentheses for each group are the total number of people per group based on the results of the Web-based questionnaire survey (thus, the numbers in each group are disparate).

3.2.1 LM (low metacognition) group (111 people)

Scores for "contemplation of the plan", "contemplation of success", and "recognition of past performance" were all low. "Anticipation and contemplation of failure" scores were about average.

3.2.2 RP (regular/realistic pessimism) group (53 people)

"Anticipation and contemplation of failure" scores were very high, and "contemplation of success" and "recognition of past performance" scores were low.

3.2.3 DP (defensive pessimism) group (213 people)

Scores for "contemplation of success" and "recognition of past performance" were higher than the standard scores.

3.2.4 RO (regular/realistic optimism) group (82 people)

"Anticipation and contemplation of failure" scores were low and other scores were higher than the standard scores.

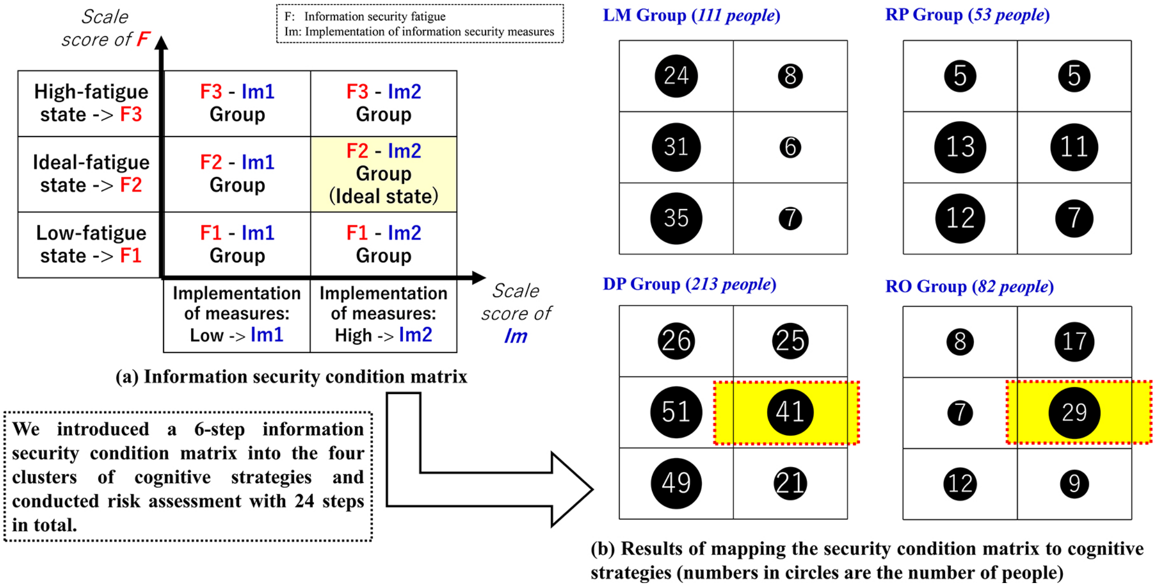
As described above, the results of the cluster analysis of this Web-based questionnaire survey showed that it can be classified into four clusters, the same as Table 1, which was cognitive strategy by Toyama's previous study. In the next section, we propose a new information security fatigue countermeasure by combining the results, i.e., the cognitive strategy classification in Table 1, with the information security condition matrix in 2.1.3.

4 Proposal and evaluation of information security fatigue countermeasures using cognitive strategy scale based on web questionnaires

In this section, information security fatigue countermeasures based on cognitive strategies and information security condition matrices in accordance with the results of Section 3 are described. Specifically, we show the results of risk assessment for 24 categories, where six categories of the information security condition matrix are mapped to each of the four categories of cognitive strategies. In other words, by adding a cognitive strategy to the classification, we newly proposed more detailed risk assessment and security countermeasures.

4.1 Proposal and evaluation of information security fatigue countermeasures

The results of mapping the Web-based questionnaire responses to the information security condition matrix in Fig. 2 for each of the four clusters of cognitive strategies in Table 1 are shown in Fig. 5. We can see that the cognitive strategy pattern in the ideal state of information security fatigue (F2-Im2 group) in Fig. 5(a) was most common in the DP group (41 participants), followed by the RO group (29 participants), as shown in Fig. 5(b).



(a) Information security condition matrix

We introduced a 6-step information security condition matrix into the four clusters of cognitive strategies and conducted risk assessment with 24 steps in total.

(b) Results of mapping the security condition matrix to cognitive strategies (numbers in circles are the number of people)

Figure 5: Mapping results of the information security condition matrix for the cognitive strategy group.

4.2 Proposal and evaluation of information security fatigue countermeasures based on open-ended format question of Web questionaries

We also conducted a risk assessment based on the results of the Web-based questionnaire for 24 categories (= 6 categories (security condition matrix classification) × 4 clusters (cognitive strategy classification)). The risk assessment was conducted using free responses to the Web-based questionnaire to analyze information security fatigue in information security measures. The question was as follows.

– *In which cases do you feel exhausted by the information security measures?*

We then came up with ways to solve the problems uncovered by the answers to the above question. In considering these measures, the results of the assessment of our previous study [6] were used as a basis. The results are presented below.

4.2.1 LM (low metacognition) group: 111 participants

The LM group consists of individuals who do not know how they are viewed by others and are not able to produce good results. First, we show the free responses to the aforementioned information security fatigue question for each classification in the information security condition matrix (F1-Im1, F1-Im2, etc.; Fig. 2).

- F1-Im1: The individuals in this group have both low metacognitive ability and low information security fatigue and are not able to take security measures. The main responses to the question of information security fatigue in this group were “Security is different depending on the position”, “It is inconvenient to ask my boss to disclose every security measure”, and “When I am instructed to take a security measure when my work is busy”.

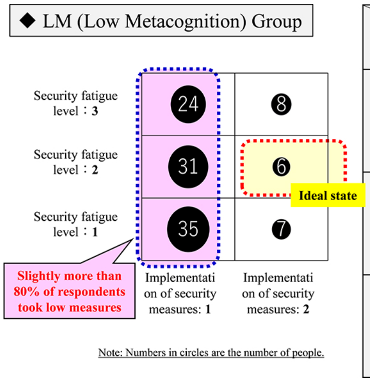
- F1-Im2: The individuals in this group have both low metacognitive ability and low information security fatigue, but they are able to take security measures. The answers to the question of information security fatigue for this group included “When we have access security at the entrance of the company, but we also have access security for each project” and “When there are restrictions on data exchange with customers”. In other words, they follow the rules, but the rules increase the level of information security fatigue.

- F2-Im1: The individuals in this group have low metacognitive ability, moderate information security fatigue, and take no security measures. The main responses to the information security fatigue question for this group were related to passwords, as seen in the responses “Frequent password changes” and “When I have to change my password”. Another 14 respondents answered “Nothing in particular”, which may be related to the fact that the level of information security fatigue in this group is moderate.

- F2-Im2: The individuals in this group have a low level of metacognition, and the levels of information security fatigue and security measures implementation are both in the ideal state. The main answer to the question of information security fatigue for this group was “Having to keep up to date”, and they maintain a moderate level of tension in order to implement security measures well.

- F3-Im1: The individuals in this group have low metacognitive ability, high information security fatigue, and take no security measures. The main answers to the question of information security fatigue for this group were “Too many internal rules”, “Every time a problem occurs in the company, the number of inconvenient rules increases and the time and effort only increases”, “In reality, the number of troublesome rules increases and they do not function”, and “When new security measures are introduced”. As indicated in the responses “Every time a new security measure is introduced, the number of troublesome rules increases”, “In reality, the number of troublesome rules increases and the system does not function”, and “When a new security measure is introduced”, there was a tendency to fall into the vicious cycle (Fig. 1).

- F3-Im2: The individuals in this group have low metacognitive ability and high levels of both information security fatigue and security measures implementation. The main answer to the question of information security fatigue for this group was that they focused on passwords (in three cases), and there were two cases where they answered that they did not have any


◆ LM (Low Metacognition) Group
Security fatigue level：3
Security fatigue level：2
Security fatigue level：1
24
8
31
6
35
7
Ideal state
Slightly more than 80% of respondents took low measures
Implementation of security measures: 1
Implementation of security measures: 2
Note: Numbers in circles are the number of people.

Security fatigue level \ Implementation of security measures	1	2
3	Since they are dissatisfied with the current security measures, it may be beneficial to conduct interview about the information security measures.	Since they might not be aware of their level of security fatigue, it may be effective to conduct interviews about the information security measures to relieve stress.
2	Although there is recognition of the importance and necessity of the measures, it may be beneficial to provide information about security solutions due to the lack of implementation of security measures.	Since this is an ideal state, it is important to let the people know they are in an ideal state and to ensure their motivation to maintain it.
1	In this group, since the lack of awareness of the parties involved needs to be addressed, education that arouses their awareness may bring them closer to the ideal state. In addition, security education is also effective because of the lack of correct knowledge about security.	Due to the uncertainty about security, active measures by individuals may also be useful. In addition, when the security measures are breached, it would be beneficial to implement motivation recovery measures after an incident occurs.

Figure 6: Proposal and evaluation of security measures for LP group.

particular answer. The main characteristic of the LM group as a whole is that they cannot look at themselves objectively, and they may not be aware of their own information security fatigue.

Next, Fig. 6 shows the results of investigating the main countermeasures based on the results of the aforementioned Web questionnaire. We can see that this LM group was characterized by a low percentage of information security fatigue in the ideal state (about 5%). In contrast, the percentage with low security measures implementation was high, at about 81%. The main measures include the provision of information security solutions and education to raise awareness of the parties involved.

4.2.2 RP (regular/realistic pessimism) group: 53 participants

The RP group consists of individuals who think everything is bad and have a gloomy outlook on the future. First, we show the free responses to the aforementioned information security fatigue question for each classification in the information security condition matrix (F1-Im1, F1-Im2, etc.; Fig. 2).

- F1-Im1: The individuals in this group are pessimistic, have low information security fatigue, and are not able to take security measures. The main answer to the question of information security fatigue for this group was “When I receive a virus mail, I feel that I should pay more attention to security”. Although they felt the need for information security measures, they did not take any.

- F1-Im2: The individuals in this group are pessimistic and have a low level of information security fatigue, but they are able to take security measures. The main answer to the question of information security fatigue in this group was “When an error occurs and I cannot solve it by myself”, indicating a tendency to leave things to others.

- F2-Im1: The individuals in this group are pessimistic, have a medium level of information security fatigue, and are not able to take security measures. The main answers to the information security fatigue question for this group indicated a tendency of lacking a sense of ownership, as seen in the answers “When the PC suddenly stops working” and “When the PC runs in the background and is slow”. In addition, there was a lack of knowledge about security, as seen in the responses “When things don’t work according to the procedure” and “Complicated settings”.

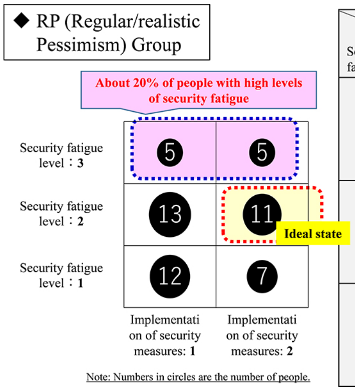
- F2-Im2: The individuals in this group are pessimistic, and the degree of information security fatigue and the degree of implementation of security measures are both in the ideal state. The main answers to the question of information security fatigue for this group were “I have to re-install a set of security measures when I replace my PC or OS”, “I feel very tired because my work does not progress even if I implement the measures”, and “I feel very tired because

I have to log in every time I use special software". These responses were followed by "I feel very tired because I have to log in every time I use the dedicated software". These responses indicate that the time consumed by security measures seems to be a cause of fatigue.

- F3-Im1: The individuals in this group are pessimistic, have a high level of information security fatigue, and are not able to take security measures. The main answers to the information security fatigue question of this group show that they have low security awareness but high information security fatigue, as seen in the answers "Setting passwords, prohibiting access except for designated individuals, etc." and "The need to fill out a control book even when taking out a single USB". These responses indicate that security awareness is low but information security fatigue is high. In addition, there was a response of "I don't know what to do", which suggests a lack of knowledge is the reason for the fatigue.

- F3-Im2: The individuals in this group are pessimistic, and both the level of information security fatigue and the level of security measures implementation are high. The main answers to the question of information security fatigue for this group were "I have to resend my password after sending an e-mail with an attached file" and "When I have to spend a lot of time due to unexpected issues such as installation of countermeasure software". This shows that although they are taking security measures, they are also suffering from information security fatigue.

Next, Fig. 7 shows the results of investigating the main countermeasures based on the results of the aforementioned Web questionnaire. As we can see, this RP group was characterized by an ideal information security fatigue state of about 21%. On the other hand, the percentage of high information security fatigue was relatively low, at about 19%. The main measures include simplified information security training and simulation exercises of information security incidents.


◆ RP (Regular/realistic Pessimism) Group
About 20% of people with high levels of security fatigue
Security fatigue level：3
Security fatigue level：2
Security fatigue level：1
5
5
13
11
Ideal state
12
7
Implementation of security measures: 1
Implementation of security measures: 2

Note: Numbers in circles are the number of people.

Security fatigue level \ Implementation of security measures	1	2
3	This group is doubtful or dissatisfied with the security measures. Therefore, it may be beneficial to help them recognize the necessity of security measures by using simulated information security incidents and to present the recommended environment for information security solutions.	Hearings about the information security measures may be beneficial to combat security fatigue. It may also be beneficial to simplify the information security training.
2	This group has a lack of knowledge about security measures. Therefore, it may be beneficial to implement self-checking with a checklist of information security measures and to provide information about security solutions.	Although this is an ideal state, they tend to feel overwhelmed by the amount of time spent on security measures, so we should try to maintain the current state by relieving stress through meetings on information security measures.
1	This group understands the need for information security measures but does not implement them. Therefore, it may be beneficial to educate them in ways that arouse their awareness of the need for information security and to conduct exercises to simulate information security incidents.	In this group, security measures are left to others and they lack any awareness of being a party to the problem. Therefore, it would be beneficial to educate them to raise their awareness.

Figure 7: Proposal and evaluation of security measures for RP group.

4.2.3 DP (defensive pessimism) group: 213 participants

The DP group consists of individuals who have positive perceptions of past performance but set low expectations for the future. First, we show the free responses to the aforementioned information security fatigue question for each classification in the information security condition matrix (F1-Im1, F1-Im2, etc.; Fig. 2).

- F1-Im1: The individuals in this group are defensively pessimistic and have a low level of information security fatigue. The main answers to the information security fatigue question for this group were "When I am told to change my password regularly" and "When I have to download software for each device". These answers indicate a tendency to take security measures only out of a sense of obligation.

- F1-Im2: The individuals in this group are defensively pessimistic and have a low level of information security fatigue but are able to take security measures. The main answers to the question of information security fatigue for this group were “When regular education is provided” and “When I am forced to frequently update password settings that are longer than necessary”, indicating that they tended to be dissatisfied despite their high level of security measures implementation.

- F2-Im1: The individuals in this group are defensively pessimistic, have a medium level of information security fatigue, and are not ready for security measures. The main answers to the question of information security fatigue for this group were “When I am made to read compliance rules” and “I feel it is tedious and tiring because I have to take courses via e-Learning on a regular basis”. These responses indicate that the respondents tended to be dissatisfied with the regular security training.

- F2-Im2: The individuals in this group are defensively pessimistic, and the degree of information security fatigue and the degree of implementation of security measures are in the ideal state. The main responses of this group to the question of information security fatigue were “When my boss and colleagues don’t understand the importance of information security” and “Being asked to take unnecessary measures by bosses with insufficient knowledge”, revealing a tendency for these respondents to feel weary due to the lack of security knowledge of the people around them. There was also a tendency to get tired of the increase in their own workload due to security measures.

- F3-Im1: The individuals in this group are defensively pessimistic, have a high level of information security fatigue, and do not take any security measures. The main responses of this group to the question of information security fatigue were “When a person with insufficient security knowledge accidentally opens a dangerous Web site” and “When investigating information security measures for affiliated companies”. These responses show there was a tendency to be affected by problems caused by differences in the security awareness of the people around them.

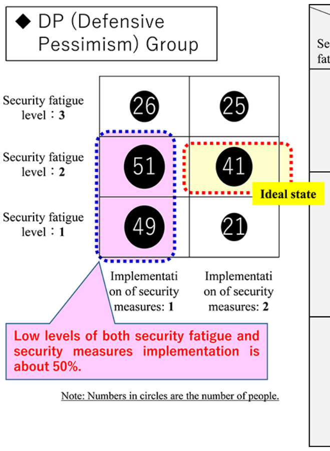
- F3-Im2: The individuals in this group are defensively pessimistic, and both the level of information security fatigue and the level of implementation of security measures are high. The main answers to the information security fatigue question for this group were “To investigate the cause of the problem and to consider and take countermeasures, such as when something actually happens” and “When I have to change all my passwords due to the effects of hacking, etc.”. These responses show there was a tendency for the respondents to always assume what would happen in the event of actual damage.

Next, Fig. 8 shows the results of investigating the main countermeasures based on the results of the aforementioned Web questionnaire. This DP group was characterized by an ideal information security fatigue state of about 19%, and the percentages of both information security fatigue and countermeasures implementation were low (about 47%). The main measures are the development of a systematic training system and a simulation exercise of information security incidents.

4.2.4 RO (regular/realistic optimism) group: 82 participants

The RO group consists of individuals who have an all-around positive outlook on things and a bright outlook on the future. First, we show the free responses to the aforementioned information security fatigue question for each classification in the information security condition matrix (F1-Im1, F1-Im2, etc.; Fig. 2).

- F1-Im1: The individuals in this group are optimistic and have a low level of information security fatigue. The main answers to the question of information security fatigue in this group tended to concern a lack of knowledge about security measures, as seen in the answers “When many screens appear on the computer” and “When things do not go smoothly for some


◆ DP (Defensive Pessimism) Group
Security fatigue level：3
Security fatigue level：2
Security fatigue level：1
26
25
51
41
49
21
Ideal state
Implementation of security measures: 1
Implementation of security measures: 2
Low levels of both security fatigue and security measures implementation is about 50%.
Note: Numbers in circles are the number of people.

Security fatigue level \ Implementation of security measures	1	2
3	In this group, security fatigue is increasing due to the difference in security awareness, so it may be beneficial to make the information security measures manual and to develop a systematic education system. It is also important to conduct meetings on the information security measures.	This group imagines what will happen if an incident actually occurs. Therefore, we should be able to reduce security fatigue by implementing motivation recovery measures after an incident and by conducting interviews on information security measures to relieve stress.
2	For a group of people who are tired of routine measures, we evoke individual active measures that do not rely on solutions. In addition, since there is a sense of mistrust related to the security measures, it may be beneficial to provide information security measures and solutions in addition to simulated exercises and recommended environments for information security solutions.	This group is in an ideal state, but they are fatigued by the difference in awareness of security measures between themselves and the people around them. Therefore, we can maintain the ideal state by equalizing the level of awareness of security measures through the development of a systematic education system. It may also be beneficial to communicate the fact that they are in the ideal state as a way of trying to maintain their motivation.
1	It is necessary to educate people to arouse their sense of ownership. In addition, since there is a sense of obligation, specific instructions on the information security measures can improve the implementation of security measures. It may also be effective to implement measures to recover motivation through education and other means when an incident occurs.	Since the measured security fatigue level is low, although they feel tired of the routine security measures, this could be improved by implementing active individual measures that do not rely on solutions and by setting up self-checking with a checklist of information security measures.

Figure 8: Proposal and evaluation of security measures for DP group.

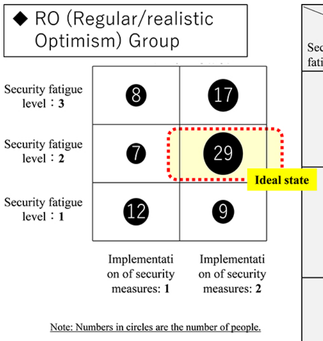
reason without my knowing why". In addition, there was a tendency to leave things to others, as seen in the response "I don't feel much fatigue because the Information System Department takes care of everything during work hours".

- F1-Im2: The individuals in this group are optimistic, have a low level of information security fatigue, and are able to take security measures. The main answers to the question of information security fatigue for this group were "It is inconvenient when I work at home because I can't take out either my personal information or information in my computer as external data" and "When I have trouble logging in due to the security rules of the company". These answers indicate that the respondents tended to feel stressed when things did not proceed as they wished.

- F2-Im1: The individuals in this group are optimistic, have a medium level of information security fatigue, and do not take any security measures. The main answers to the question of information security fatigue for this group were "When updating anti-virus software", "When sending files to the outside, I cannot send them immediately due to the security function", and "When I have to log in to my computer repeatedly if I leave my seat frequently". These responses indicate there was a tendency to think that the security measures themselves were excessive.

- F2-Im2: The individuals in this group are optimistic, and the level of information security fatigue and the level of implementation of security measures are in the ideal state. The main answers to the question of information security fatigue for this group were "When the company forces me to take measures that I think are ineffective", "When it is troublesome to update passwords regularly", and "When I am forced to monitor and follow up on sloppy data storage or attempts to take out data by people with low security awareness in the company". These responses indicate that there was a tendency to get tired of unnecessary work due to differences in knowledge and awareness of security. In addition, there was one answer that was typical of the RO group: "If it becomes a habit, I do not feel any particular burden".

- F3-Im1: The individuals in this group are optimistic, have a high level of information security fatigue, and are not able to take security measures. The main answer to the question of information security fatigue for this group was "When I try to set up the system as described but it does not work as it should". This response indicates that those with higher levels of information security fatigue tended to have insufficient security knowledge. There was also a tendency to think of security measures as a necessary evil, as in "I cannot get work done because I am too focused on security".


◆ RO (Regular/realistic Optimism) Group
Security fatigue level：3
Security fatigue level：2
Security fatigue level：1
8
17
7
29
12
9
Ideal state
Implementation of security measures: 1
Implementation of security measures: 2
Note: Numbers in circles are the number of people.

Implementation of security measures / Security fatigue level	1	2
3	This group is experiencing security fatigue due to a lack of security knowledge. We should be able to solve this problem by providing specific instructions on the content of information security measures and by presenting the recommended environment for information security solutions.	In this group, the low awareness of security measures is evident. We should be able to raise the awareness of the parties involved through education. It may also be beneficial to provide information security solutions to increase their awareness.
2	This group thinks the current security measures are excessive. We should be able to improve the implementation of security measures by presenting the recommended environment for information security solutions.	Although this group is in an ideal state, the difference in security awareness between themselves and the people around them is expressed as security fatigue, and therefore, a systematic education system needs to be developed. We should also be able to present more advanced security measures, since the people in this group already have a high awareness of security measures.
1	Since this group shows a lack of knowledge about security, we may be able to compensate for this lack by providing specific instructions on information security measures and providing information security solutions. In addition, due to the tendency of this group to leave security measures to others, it may be beneficial to provide education to arouse the awareness of the parties involved.	This group does not have a high degree of awareness of the parties involved in the security measures. Therefore, it may be beneficial to use education to arouse their consciousness of the security measures or have them experience a simulated information security incident.

Figure 9: Proposal and evaluation of security measures for RO group.

- F3-Im2: The individuals in this group are optimistic and have a high level of information security fatigue and security measure implementation. The main answers to the question of information security fatigue for this group were “In case of inaccessibility due to forgetting to change the security password” and “Troublesome due to regular password changes”. These responses indicate that, although the degree of implementation of security measures was high, there was a tendency to think that password measures were a bother.

Next, Fig. 9 shows the results of investigating the main countermeasures based on the results of the aforementioned Web questionnaire. This RO group was characterized by a relatively high percentage of information security fatigue in an ideal state (about 32%) and a high percentage of security implementation measures (about 61%). The main measures include education to improve the awareness of the parties involved and the provision of information security solutions.

5 Conclusion and future work

In this paper, we have introduced a new cognitive strategy to enable detailed countermeasures against information security fatigue from a psychological point of view. Specifically, we proposed a cognitive strategy consisting of four cognitive patterns as a countermeasure for the psychological aspect of information security fatigue. The proposed cognitive strategy makes it possible to assume 24 behavioral patterns, in contrast to the six classifications based on the conventional information condition matrix, and enables the planning of more detailed information security fatigue countermeasures. As our proposed method contributes to detailed countermeasures to be taken against information security fatigue, it is expected to reduce security incidents such as information leakage due to internal fraud.

In future work, we will investigate more concrete measures against information security fatigue that consider cognitive strategy groups, such as applications to team building.

Acknowledgemnt

This work was supported by JSPS KAKENHI Grant Number JP 19H04098.

References

[1] Methodology: Online research（conducted using macromill’s panel).

[2] N. Cantor et al. Life tasks, self-concept ideals, and cognitive strategies in a life transition. *Journal of Personality and Social Psychology*, 53:1178–1191, 1987.

[3] T. Hatashima et al. Study on visualization of information security fatigue in university students. pages 888–895. CSS2017: Computer Security Symposium 2017 (Japanese Edition), IPSJ, 2017.

[4] T. Hatashima et al. Evaluation of the effectiveness of risk assessment and security fatigue visualization model for internal e-crime. pages 707–712, Tokyo, July 2018. 42nd IEEE International Conference on Computer Software & Applications (SAPSE2018).

[5] T. Hatashima et al. Proposal of information security fatigue countermeasures for college students by improved information security condition matrix. *IPSJ Journal (Japanese Edition)*, 59(12):2105–2119, 2018.

[6] T. Hatashima et al. A proposal of information security fatigue scale (university student edition) —design and evaluation of measurement method using the way of thinking of burnout scales—. *IEICE Trans. Inf. & Syst. (Japanese Edition)*, J101-D(10):1414–1426, Oct. 2018.

[7] T. Hatashima et al. Development of security fatigue scale (SFS-9) and investigation of the reliability and the validity). *IPSJ Journal (Japanese Edition)*, 61(9):1472–1485, 2020.

[8] R. Hirano et al. Secure and effective password management system. *IEICE Technical Report (Japanese Edition)*, 111(286):129–134, 2011.

[9] it mint.com. Cluster analysis using the “ward” method. `https://it-mint.com/2017/09/23/hierarchical-clustering-ward-method-1238.html`, 2017.

[10] JNSA. 2017 investigation report on information security incidents, (japanese edition). `https://www.jnsa.org/result/incident/data/2017incident_survey_sokuhou_ver1.1.pdf`, 2018.

[11] M. Mitsunami. The effects of different cognitive strategies on the adoption of self-handicapping and stress management strategies—categorization of the four cognitive strategies in academic situations. *THE JAPANESE JOURNAL OF PERSONALITY (Japanese Edition)*, 19(2):157–169, 2010.

[12] NIST. ‘security fatigue’ can cause computer users to feel hopeless and act recklessly, new study suggests. `https://www.nist.gov/news-events/news/2016/10/security-fatigue-can-cause-computer-users-feel-hopeless-and-act-recklessly`, 2016.

[13] J. K. Norem et al. Anticipatory and post hoc cushioning strategies: Optimism and defensive pessimism in “risky” situations. *Cognitive Therapy and Research*, 10:347–362, 1986.

[14] M. Ogawa et al. Information security fatigue countermeasures based on cognitive strategy scale. pages 362–367. 2020 Eighth International Symposium on Computing and Networking Workshops (CANDARW), 2020.

[15] Parkin et al. Applying cognitive control modes to identify security fatigue hotspots, symposium on usable privacy and security (soups 2016). Retrieved from `https://www.usenix.org/conference/soups2016/workshopprogram/wsf/presentation/parkin`.

[16] S. Tanimoto et al. A concept proposal on modeling of security fatigue level. pages 29–34. ACIT2017: 5th International Conference on Applied Computing & Information Technology, 2017.

[17] M. Toyama. Reliabity and validity of the cognitive strategy scale. *Japanese Journal of Educational Psychology (Japanese Edition)*, 63(1):1–12, 2015.