2022 12th International Congress on Advanced Applied Informatics (IIAI-AAI) | 978-1-6654-9755-8/22/$31.00 ©2022 IEEE | DOI: 10.1109/IIAIAAI55812.2022.00115

A Study of Risk Assessment Quantification for Secure Telework

Hiroki Koyama
Faculty of Social System Science
Chiba Institute of Technology
Chiba, Japan
hiroki.koyama15@gmail.com

Yuuna Nakagawa
Faculty of Social System Science
Chiba Institute of Technology
Chiba, Japan
s1842095JQ@s.chibakoudai.jp

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

Teruo Endo
Faculty of Liberal Arts Osaka
Shoin Women's University
Osaka, Japan
endo.teruo@osaka-shoin.ac.jp

Takashi Hatashima
NTT Social Informatics
Laboratories
Musashino, Japan
takashi.hatashima.ch@hco.ntt.co.jp

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

***Abstract*— In Japan, telework is attracting renewed attention due to the government-led "work style reform". The advent of COVID-19 in 2020 has led to the rapid spread of telework, and the current state of widespread use may be attributed to transient factors as a counter to the spread of COVID-19 infection. A current problem is that dealing with the emergence of risks has been postponed or overlooked because telework was hastily promoted and introduced even though sufficient preparations had not been made. In this work, we conducted a risk assessment from the viewpoints of both companies and employees to identify 28 risk factors and proposed countermeasures for these factors in order to make teleworking permanently safe and secure in the new normal era. The results revealed that the introduction of Mobile Device Management (MDM) to teleworking terminals is effective as the main countermeasure on the corporate side. The study also clarified that the establishment of various systems related to the telework environment and the use of cloud computing are effective as measures for both companies and employees. We also evaluated the effectiveness of the proposed risk measures in terms of risk values and found that these could be reduced by approximately 61%. Our findings will contribute to the safe and secure use of telework in the new normal era.**

Keywords*— *Telework, Work Style Reform, Risk Assessment

I. Introduction

Telework is a work style that enables people to work regardless of time and place through the use of Information and Communication Technology (ICT). In general, there are three major types of telework telecommuting, in which work is performed at home without going to the office; mobile work, in which work is performed on the road or in cafes; and satellite work, in which work is performed in offices other than the workplace [1].

Telework has undeniable advantages for both employees and companies. The benefits for employees include an improved work-life balance and a reduction in commuting fatigue, while the benefits for companies are the assurance of business continuity in the event of a disaster or pandemic and a reduction in the number of employees who take time off work due to childcare or nursing care, thereby securing the workforce [2]. As mentioned above, the need for telework as a measure to prevent the spread of COVID-19 infection has also increased in recent years and is spreading rapidly.

However, the problem with telework is that risks that have been postponed or overlooked are now more become apparent, as telework was hastily promoted even though companies were not yet ready for it in terms of their systems.

In this paper, we report the risk assessment we conducted based on the perspectives of both the company and the employees (i.e., the stakeholders) in order to utilize telework in a safe and secure manner on a permanent basis in the new normal era. Specifically, using past literature and case studies as a basis, we first comprehensively extracted risk factors in teleworking using the Risk Breakdown Structure (RBS) method. Next, we analyzed the extracted risk factors using the risk matrix method, and proposed countermeasures for these factors. Finally, we evaluated the proposed countermeasures terms of risk values.

Section 2 of this paper describes the current status and issues of telework. We discuss related work in Section 3, and in Section 4, based on the results of Sections 2 and 3, we discuss our assessment of risk factors in telework. Section 5 presents our conclusions and touches on future issues.

978-1-6654-9755-8/22/$31.00 ©2022 IEEE
DOI 10.1109/IIAIAAI55812.2022.00115

II. CURRENT STATUS AND ISSUES OF TELEWORK

A. Current Status of Telework

In recent years, government-led “work style reforms” have been promoted in Japan, which has led to the requirement of more flexible work styles. Among these, teleworking has been attracting attention because it enables people to work without being restricted by time or place through the use of ICT. For example, it can be used to secure the labor force in an aging society with a declining birthrate by reducing job turnover due to childcare and nursing care and by increasing job opportunities for the elderly and physically challenged people who have difficulty commuting to work. According to a survey by the Ministry of Internal Affairs and Communications (MIC), the number of companies responding that they have already introduced telework has been increasing over the past 15 years, from 8.5% in 2004 to 21.1% in 2019, but it is not yet widespread [3].

As for other countries, the United States has the highest percentage of companies that have already introduced telework (85.0%), followed by the United Kingdom (38.2%) and Germany (21.9%) [4]. In the United States, where the rate of telework adoption is the highest, the federal government has been promoting the introduction of telework since the early 1990s, and in 2010 it enacted the Telework Enhancement Act. Telework is being actively promoted not only by private companies but also by government employees, including employees of ministries and state governments [5].

The number of companies in Japan that are trying to introduce teleworking has been rapidly increasing since the advent of COVID-19. In a survey on the introduction rate of telework conducted by the Tokyo Metropolitan Government in March and April 2020, 24.0% of respondents answered that they had introduced it in March, compared to 62.7% in April. The percentage of employees who are implementing telework was about 20% as of December, but about 50% of employees had started implementing telework as of April.

B. Issues of Telework

While telework has undeniable advantages, there are also many challenges that complicate its widespread adoption. One example is found in the “White Paper on Information and Communications 2018” published by the MIC, where the largest number of respondents indicated that the development of a telework environment is an issue. In addition, according to the answers to a questionnaire administered to companies that have introduced telework, communication among employees and system design during telework can also be considered issues, as evidenced by the introduction of web conferencing, chat, etc. along with the study necessary to introduce a new telework system that meets the needs of the new normal era [6]. In the telework work environment, it is important for employers to educate and advise employees to create an environment that takes health and safety into consideration, and to consider improving the environment or using satellite offices and other work locations outside the home. In addition, because teleworkers work in an environment where there are no supervisors or coworkers around, they cannot communicate as easily as in the traditional workplace, and mental health issues emerge, such as a sense of loneliness and difficulties in noticing mental or physical changes in employees.

III. RELATED WORK

There have been numerous studies of the risks associated with telework, both before and current with the outbreak of the COVID-19 pandemic.

According to T. Gentle [7], while the transition to telework has been rapidly progressing in the United States due to the influence of COVID-19, many companies still use the same tools and techniques as in the traditional workplace and assume that these will continues to work. Moreover, it is not enough for companies to ensure protection from the outside they also need to deal with internal threats. The risks of remote work environments need to be mitigated through employee education, virtual applications and desktops, communications, security enhancements, and user behavior analysis.

Y. Huiyi et al. [8] clarified that technological advances create new risks and solutions for telework. He pointed out that, as with other security risks, they need to be constantly updated. While telework has many advantages, it can also lead to security risks such as data leakage and falsification. However, these risks can be controlled, and several methods for doing so have been proposed, including those for establishing policies, training employees, securing networks and devices, and encrypting information.

P. Pyoria [9] attributed the slow diffusion of telework to the fact that businesses are concentrated in certain regions and a telework culture and contractual framework has not been established. He also stated that success is more likely to occur if the benefits and risks associated with telework are prepared for from the outset.

S. Desio et al. [10] evaluated the impact of teleworking as a response to COVID-19 on organizations, with a particular focus on psychological distress and well-being. Their findings showed that employees may be exposed to psychosocial risks such as loneliness, stress, and overwork, and are at risk for unhealthy eating and increased smoking, especially if they live alone.

A. M. Luchena et al. [11] analyzed teleworking form a social welfare point of view under a declared state of emergency in Spain and found that teleworking allowed for a more flexible response to COVID-19 and a more flexible work-life balance, while they pointed out that it is also necessary to consider psychological risks such as working long hours, switching between work and private life, the impact of law amendment, and technological advances. In particular, disparities with older workers and gender considerations were noted.

While these previous studies have described external and internal security risks and psychological risks, not enough research has been done on the risks of telework work environments and internal systems. In addition, in individual studies, risks on the corporate side, such as long working hours and legal changes, and risks on the employee side, such as internal fraud and psychological risks, have not been studied in an integrated manner. Moreover, as some studies have stated, risk analysis by COVID-19 impact is useful because risks need to be constantly reviewed and updated according to technological advances and the current times.

IV. RISK ASSESSMENT IN TELEWORK

A. Risk Assessment Process

Risk assessment is one of the most important steps in any risk management process. How well risks are managed depends on by anticipating them and taking measures to avoid them in advance. After referring to papers by S. Frosdick [12] and others, we decided to proceed with risk assessment in the following process: (1) risk identification, (2) risk analysis, and (3) risk evaluation.

B. Identification of Risk Factors

Here, we used the RBS method, a typical risk analysis method in project management, to comprehensively extract risk factors for telework [13]. The items to be structured using RBS were extracted from the results of three case studies [6, 14, 15] and multiple reviews by the authors form the Mutually Exclusive, Collectively Exhaustive (MECE) perspective. In addition, the validity of this review is based on the multifaceted perspectives of the authors, whose attributes include university professors, corporate researchers, and students. Table I (1) show the risk factor extraction results, where we categorized the risk factors of teleworking into both corporate and employee aspects in the first level and into environmental, security, and institutional aspects in the next level. Through this hierarchical and exhaustive study, we ultimately identified 28 risk factors. On the employee side, risk factors include the telework environment (such as the tools used in telework, the network, and the work environment) as well as psychological aspects (such as internal fraud and security, including privacy). The risk factors on the corporate side are internal rules (such as the cost of building the work environment, provision of utilities during work, and rules for telework) as well as internal systems including attendance management [16].

Table I. Risk specification results by RBS and risk analysis results by risk matrix methods

(1) Results of risk factor extraction using RBS method					(2) Results of risk analysis using risk matrix method			
No.	Level1	Level2	Level3	Level4/Risk Factor	Risk Probability	Risk Impact	Risk Classification	Risk Countermeasures
1	Employee side	Telework environment	Telework tools	Lack of proficiency with tools such as Remote Desktop	High	Low	Risk Mitigation	Create procedures for work and communication tools based on the company's security policy, and educate employees about the rules on a regular basis.
2				Lack of proficiency with communication tools such as web conferencing				
3			Working environment	Insufficient bandwidth in the network environment				Data dieting (e.g., limiting video and audio for web conferencing when bandwidth is insufficient) is performed as necessary.
4				Lack of printers and other fixtures				Establish a system for companies to pay for the construction of telework environments.
5				Vulnerability of telecommunication devices for telework	Low	High	Risk Transfference	Keep telework communication device software up to date. Manage the access log.
6				Lack of independent telework environment	High	High	Risk Avoidance	Establish a system for companies to pay for the construction of telework environments.
7				Health hazards such as economy class syndrome				Companies should develop labor management for teleworkers and ensure that they have time for health care.
8		Security environment	Physical security	Shoulder hacking into PC screen in a telework environment	High	Low	Risk Mitigation	Create telework work standards based on the company's security policy and educate employees about the rules on a regular basis.
9				Loss of corporate terminal for telework	Low	High	Risk Transfference	MDM should be implemented for company-leased terminals, and encryption should be required when storing data; for non-company-leased terminals (e.r., BYOD), remote VPN and cloud computing should be required.
10				Use of shared home terminals				Based on the company's security policy, create telework work standards, such as prohibiting the use of terminals other than company-loaned terminals and authorized terminals, and educate employees about them.
11				Use of free Wi-Fi, etc.				Companies can set up a system to pay for the construction of a telework environment and lend mobile Wi-Fi to their employees.
12				No face-to-face surveillance possible	High	High	Risk Avoidance	Companies should establish a working environment for telework and require employees to report on the progress of their work on a regular basis.
13			Cyber security	File-sharing mistakes	Low	High	Risk Transfference	Create telework work standards based on the company's security policy, and educate employees about them. Specifically, prohibit the use of terminals other than those loaned by the company or those authorized (e.g., MDM-implemented terminals), and require the use of remote VPN or cloud computing for BYOD and other non-company loaned terminals.
14				Unauthorized access				
15				Computer virus				
16				Use of outdated security software				
17				Installation of unnecessary software				
18			Psychological security	Internal fraud				Create telework work standards based on the company's security policy, and educate employees on a regular basis.
19				Lack of a face-to-face partner (loneliness while working)	High	High	Risk Avoidance	Provide a virtual environment where companies can develop a labor environment for telework and enable employees to communicate with each other.
20			Privacy	Leakage of images and conversations of non-related parties during a web conference				Create telework work standards based on the company's security policy and educate employees about them.
21				Mirroring of work area during a web conference	Low	High	Risk Transfference	Establish a system in which companies pay for the construction of a telework environment.
22	Employer side	Internal legal system	Internal rule	Fees for telework environment				
23				Inadequate communication rules in telework environment	High	Low	Risk Mitigation	Provide a virtual environment where companies can set up a working environment for teleworking and hold regular formal meetings.
24				Increase in water and electricity costs due to working in telework environment	High	High	Risk Avoidance	Establish a system in which companies pay for the construction of telework environments.
25				Mail delivered to the office addressed to a teleworking employee	High	Low	Risk Mitigation	Create telework work standards based on the company's security policy and educate employees about them.
26			Labor management	Inadequate labor management in telework	High	High	Risk Avoidance	Provide a virtual environment where companies can set up a working environment for teleworking and hold regular formal meetings.
27				Increase in overtime hours in telework		High		Companies should develop a labor environment for telework and share the management of working hours within the company, including managers.
28				Increase in web conferencing in telework	High	Low	Risk Mitigation	

C. Risk Analysis and Proposal of Countermeasures

In the risk analysis, we used the risk matrix method to capture the characteristics of telework risk as an initial study. This method is a qualitative analysis technique that classifies each risk factor into one of the four areas shown in Fig.1. As shown in Table I (2), eight risk factors were classified as Risk Avoidance, 12 as Risk Transference, eight as Risk Mitigation, and zero as Risk Acceptance. Thus, measures based on Risk Transference accounted for about half of the total.

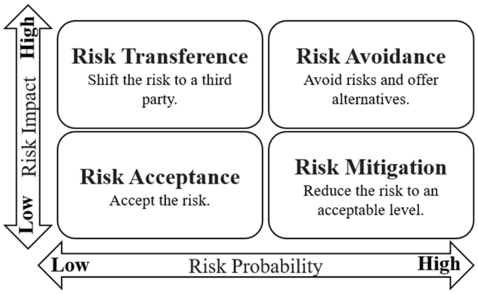


Figure 1 Risk matrix method

The following are the results of our analysis of the 28 risk factors listed in Table I using the risk matrix method.

1) *Risk Transference*

Table II lists the risk factors for which the risk classification was "Risk Transference". The main trends here include many of the security issues involved in teleworking, such as physical security, cyber security, and psychological security. The main countermeasures include the introduction of MDM for teleworking terminals, obligatory use of Virtual Private Network (VPN) and cloud computing for Bring Your Own Device (BYOD) and other terminals not leased by the company, and teleworking based on the company's security policy. The Clear standards should be developed and employees should be educated.

2) *Risk Avoidance*

Table III shows the list of risk factors whose risk classification was "Risk Avoidance". The main trends here include problems with the telework environment and attendance management. Major measures include the development of support systems for companies to establish a telework environment and the development of labor management for telework.

3) *Risk Mitigation*

Table IV shows the list of risk factors with a risk classification of "Risk Mitigation". The main trends here include problems with telework tools, telework environments, and internal company rules. The main measures include the development of a labor environment for telework and the creation of telework standards based on security policies by companies and the implementation of training for employees.

4) *Summary*

On the basis of the above results, the main risk measures for the 28 risk factors are as follows.

a) Companies create telework standards based on their security policies.

b) MDM and data encryption are installed in company-rented terminals.

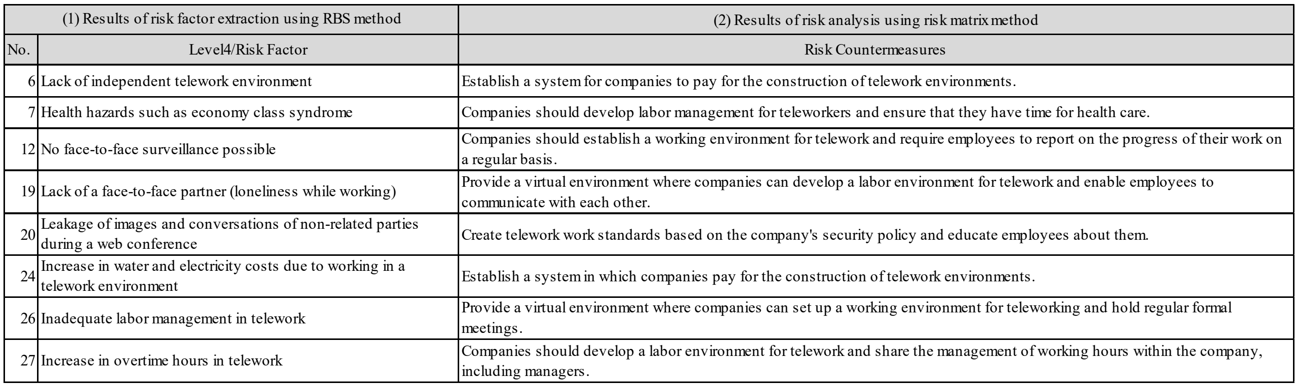
c) For terminals other than company-issued terminals (e.g., BYOD), VPN and cloud computing are obligatory [17].

The most important risk countermeasure for telework is the establishment of a telework system based on the basic corporate security policy, which includes strengthening the operational aspects of telework, i.e., working style, work environment (including tools), and security.

Table II. Risk transference measure characteristics (risk probability: low, risk impact: high)

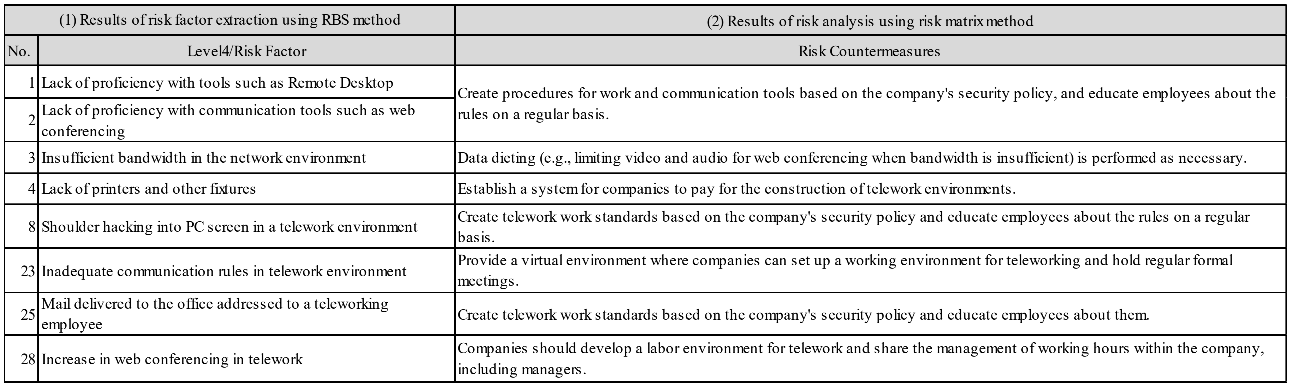
(1) Results of risk factor extraction using RBS method		(2) Results of risk analysis using risk matrix method
No.	Level4/Risk Factor	Risk Countermeasures
5	Vulnerability of telecommunication devices for telework	Keep telework communication device software up to date. Manage the access log.
9	Loss of corporate terminal for telework	MDM should be implemented for company-leased terminals, and encryption should be required when storing data; for non-company-leased terminals (e.g., BYOD), remote VPN and cloud computing should be required.
10	Use of shared home terminals	Based on the company's security policy, create telework work standards, such as prohibiting the use of terminals other than company-loaned terminals and authorized terminals, and educate employees about them.
11	Use of free Wi-Fi, etc.	Companies can set up a system to pay for the construction of a telework environment and lend mobile Wi-Fi to their employees.
13	File-sharing mistakes	Create telework work standards based on the company's security policy, and educate employees about them. Specifically, prohibit the use of terminals other than those loaned by the company or those authorized (e.g., MDM-implemented terminals), and require the use of remote VPN or cloud computing for BYOD and other non-company loaned terminals.
14	Unauthorized access	
15	Computer virus	
16	Use of outdated security software	
17	Installation of unnecessary software	
18	Internal fraud	Create telework work standards based on the company's security policy, and educate employees on a regular basis.
21	Mirroring of work area during a web conference	Establish a system in which companies pay for the construction of a telework environment.
22	Fees for telework environment	

Table III. Risk avoidance measure characteristics (risk probability: high, risk impact: high)



(1) Results of risk factor extraction using RBS method		(2) Results of risk analysis using risk matrix method
No.	Level4/Risk Factor	Risk Countermeasures
6	Lack of independent telework environment	Establish a system for companies to pay for the construction of telework environments.
7	Health hazards such as economy class syndrome	Companies should develop labor management for teleworkers and ensure that they have time for health care.
12	No face-to-face surveillance possible	Companies should establish a working environment for telework and require employees to report on the progress of their work on a regular basis.
19	Lack of a face-to-face partner (loneliness while working)	Provide a virtual environment where companies can develop a labor environment for telework and enable employees to communicate with each other.
20	Leakage of images and conversations of non-related parties during a web conference	Create telework work standards based on the company's security policy and educate employees about them.
24	Increase in water and electricity costs due to working in a telework environment	Establish a system in which companies pay for the construction of telework environments.
26	Inadequate labor management in telework	Provide a virtual environment where companies can set up a working environment for teleworking and hold regular formal meetings.
27	Increase in overtime hours in telework	Companies should develop a labor environment for telework and share the management of working hours within the company, including managers.

Table IV. Risk mitigation measure characteristics (risk probability: high, risk impact: low)



(1) Results of risk factor extraction using RBS method		(2) Results of risk analysis using risk matrix method
No.	Level4/Risk Factor	Risk Countermeasures
1	Lack of proficiency with tools such as Remote Desktop	Create procedures for work and communication tools based on the company's security policy, and educate employees about the rules on a regular basis.
2	Lack of proficiency with communication tools such as web conferencing	
3	Insufficient bandwidth in the network environment	Data dieting (e.g., limiting video and audio for web conferencing when bandwidth is insufficient) is performed as necessary.
4	Lack of printers and other fixtures	Establish a system for companies to pay for the construction of telework environments.
8	Shoulder hacking into PC screen in a telework environment	Create telework work standards based on the company's security policy and educate employees about the rules on a regular basis.
23	Inadequate communication rules in telework environment	Provide a virtual environment where companies can set up a working environment for teleworking and hold regular formal meetings.
25	Mail delivered to the office addressed to a teleworking employee	Create telework work standards based on the company's security policy and educate employees about them.
28	Increase in web conferencing in telework	Companies should develop a labor environment for telework and share the management of working hours within the company, including managers.

D. Evaluation of Risk Countermeasures by Risk Values

Next, we evaluated the effectiveness of the proposed measures by quantifying the risk factors listed in Table I. We used common risk calculation formulas in the field of ISMS, to determine risk values based the qualitative results reported above. Finally, risk values were calculated using formulas and approximations [18].

1) Ordinary Risk Value Formula

Each risk value is quantified as follows.

$$\text{Risk value} = \text{value of asset} * \text{value of threat} * \text{value of vulnerability} \qquad (1)$$

In general, calculating the elements on the right-hand side of Eq, (1) is very difficult, so to simplify, we used the following approximate formulas [19, 20, 21].

2) Approximate Risk Value Formula

2-a) Approximation of Asset Value

The asset value is approximated by the impact of the risk matrix, as shown in Fig.2. In other words, the value of an asset is considered to be the impact of risk. Degrees of risk are defined as 1 (low) to 5 (high) [19]. The risk matrix is divided into two risk impact levels, where for the sake of simplicity, the higher impact is assumed to be 5 (the maximum risk level) and the lower impact is assumed to be 1 (the minimum risk level).

2-b) Approximation of Threat Value

The threat value in Eq. (1) is approximated by the risk occurrence probability in the risk matrix. In the reference literature, risk probability is defined in three levels [19]. These values are mapped to the risk occurrence probabilities in the risk matrix in Fig.2, (as in a above), with the maximum value of the risk occurrence probability being 3 and the minimum value being 1.

2-c) Approximation of Value of Vulnerability

The vulnerability rating is defined as a three-level rating: 3 (high), 2 (medium), and 1 (low) [19]. Here, the four regions in Fig.2 are classified into three categories according to risk probability and risk impact. Risk Avoidance is approximated as 3 (high), Risk Transference and Risk Mitigation as 2 (medium), and Risk Acceptance as 1 (low). As described above, Eq. (1) can be approximated as in Eq. (2). Approximate values for each parameter in Eq. (2) are listed in Table V.

$$\text{Risk value} \fallingdotseq \text{value of risk impact} * \text{value of risk probability} * \text{value of vulnerability} \qquad (2)$$

3) Calculation of Risk Value Based on Eq. (2)

We calculated risk values for all risk factors using Eq. (2). Then, we implemented the proposed countermeasures and calculated the risk values again. The results are shown in Table VI.

Table V. Approximate values of Eq. (2)

	Risk Impact	Risk Probability	Vulnerability	
High	3	5	Risk Avoidance	3
Low	1	1	Risk Transference and Mitigation	2
			Risk Acceptance	1

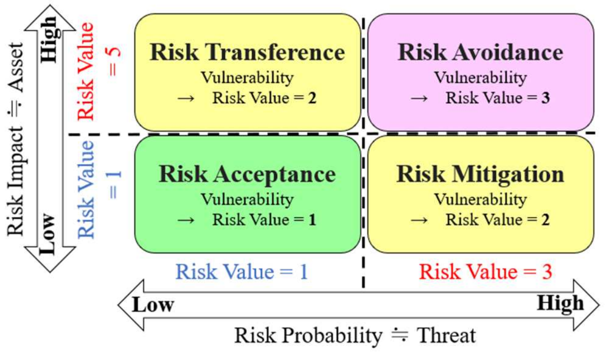


Figure 2 Risk value approximation of risk matrix

Table VI. Risk analysis results

No.	Risk Factor	Risk Probability	Risk Impact	Before risk countermeasures		After risk countermeasures	
				Vulnerability (Risk Classification)	Risk value	Vulnerability (Risk Classification)	Risk value
1	Lack of proficiency with tools such as Remote Desktop	3	1	2	6	1	3
2	Lack of proficiency with communication tools such as web conferencing	3	1	2	6	1	3
3	Insufficient bandwidth in the network environment	3	1	2	6	1	3
4	Lack of printers and other fixtures	3	1	2	6	1	3
5	Vulnerability of telecommunication devices for telework	3	5	2	30	1	15
6	Lack of independent telework work environment	3	5	3	45	1	15
7	Health hazards such as economy class syndrome	3	5	3	45	1	15
8	Shoulder hacking into the PC screen in a telework environment	3	1	2	6	1	3
9	Loss of corporate terminal for telework	1	5	2	10	1	5
10	Use of shared home terminals	1	5	2	10	1	5
11	Use of free Wi-Fi, etc.	1	5	2	10	1	5
12	No face-to-face surveillance possible	3	5	3	45	1	15
13	File sharing mistakes	1	5	2	10	1	5
14	Unauthorized access	1	5	2	10	1	5
15	Computer virus	1	5	2	10	1	5
16	Use of outdated security software	1	5	2	10	1	5
17	Install unnecessary software	1	5	2	10	1	5
18	Internal fraud	1	5	2	10	1	5
19	Lack of a face-to-face partner (loneliness while working)	3	5	3	45	1	15
20	Leakage of images and conversations of non-related parties during a web conference	3	5	3	45	1	15
21	Mirroring of the work area during a web conference	1	5	2	10	1	5
22	Fees for telework environment	1	5	2	10	1	5
23	Inadequate communication rules in a telework environment	3	1	2	6	1	3
24	Increase in water and electricity costs due to working in a telework environment	3	5	3	45	1	15
25	Mail delivered to the office addressed to a teleworking employee	3	1	2	6	1	3
26	Inadequate labor management in telework	3	5	3	45	1	15
27	Increase in overtime hours in telework	3	5	3	45	1	15
28	Increasing Web Conferencing in Telework	3	1	2	6	1	3
				Risk value (total)	**548**	Risk value (total)	**214**

Table VII shows the percentage of reduction in risk values after implementing the countermeasures. As we can see, the overall risk reduction was about 61%. This demonstrates that the proposed measures are effective despite the fact that the risk value is a relative measure.

Table VII. Percentage of reduction in risk value

	Before risk countermeasures (1)	After risk countermeasures (2)
Risk value (total)	548	214
Risk value reduction rate = ((1)-(2))/ (1)	—	0.61

V. CONCLUSION AND FUTURE WORK

In this paper, we conducted a risk assessment of telework based on the perspectives of both companies and employees in order to utilize telework permanently, safely, and securely in the new normal era. Specifically, we comprehensively extracted 28 risk factors using the RBS method, analyzed them, and proposed countermeasures. Our analysis revealed eight risk factors in the Risk Avoidance category, 12 in Risk Transference, eight in Risk Mitigation, and zero in Risk Acceptance. Thus, measures based on Risk Transference accounted for about half of the total. Our findings clarified that the most important thing is to strengthen the operational aspect of telework, i.e., to establish a telework system based on the company's security policy. The effectiveness of the proposed risk countermeasures was also clarified through an evaluation by risk values, where we found that the risk value after implementation of the countermeasures was reduced by approximately 61%. These results will contribute to the safe and secure use of telework in the new normal era.

Our future work will include conducting risk assessments of telework based on management perspectives and evaluating the cost-effectiveness of risk countermeasures.

ACKNOWLEDGMENT

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

REFERENCES

[1] Y. Ide, "A case of officework (Telework)", Ergonomics, Vol. 55 Supplement Issue, S2F2-4, Japan Human Factors and Ergonomics Society, 2019(Japanese Edition)

[2] T. Kamei, et al., "Challenges and prescriptions for reforming work styles through telework", Knowledge of Asset Creation, July 2017 issue, pp.36-49, NRI, 2017, (Japanese Edition)

[3] Ministry of Internal Affairs and Communications, "2019 Report on the Survey of Telecommunications Usage Trends (Enterprise Edition)", 2019, https://www.soumu.go.jp/johotsusintokei/statistics/pdf/HR201900_002.pdf, (accessed 2022/05/26), (Japanese Edition)

[4] Ministry of Health, Labour and Welfare, "Telework Portal Site Overseas Initiatives", https://telework.mhlw.go.jp/telework/abr/, (accessed 2021/03/04) , (Japanese Edition)

[5] M. Furuya, "World telework situation 2012", Japan Telework Society, The 13th Academic Salon, https://www.mlit.go.jp/crd/daisei/telework/docs/H24b_06.pdf, (accessed 2021/03/04) , (Japanese Edition)

[6] Ministry of Internal Affairs and Communications, "Realizing a comfortable workplace through telework", 2021, https://www.soumu.go.jp/johotsusintokei/statistics/pdf/HR201900_002.pdf, (accessed 2022/05/26), (Japanese Edition)

[7] T. Gentle, "Insider Threat Risk Assessment and Telework", ED-520: Foundations of Insider Threat Management, https://securityawareness.usalearning.gov/cdse/itawareness/documents/TorielloK-NITAM-Essay.pdf, (accessed 2022/05/26), 2021

[8] Y. Huiyi, et al., "Security Risks in Teleworking:A Review and Analysis", The University of Melbourne, https://minerva-access.unimelb.edu.au/items/c37178db-9b3c-5ff6-89b9-8f264b789555, (accessed 2022/05/26), 2013

[9] P. Pyoria, "Managing telework: risks, fears and rules", Management Research Review, Vol. 34 No. 4, pp. 386-399.,2011

[10] S.Desio, et al., "Telework and its effects on mental health during the COVID-19 lockdown", European Review for Medical and Pharmacological Sciences, 25, pp.3914-3922, 2021

[11] A. M. Luchena, et al., "Telework and Social Services in Spain during the COVID-19 Pandemic", Int. J. Environ. Res. Public Health 2021, 18, 725, 2021

[12] S. Frosdick, "The techniques of risk analysis are insufficient in themselves", Disaster Prevention and Management, Disaster Prevention and Management, Vol. 6, No. 3, pp. 165–177, 1997

[13] Manick, "Risk Breakdown Structure", http://www.justgetpmp.com/2011/12/risk-breakdown-structure-rbs.html, (accessed 2022/05/22)

[14] Sky , "Awareness Survey on Telework", https://www.skygroup.jp/news/201019_01/, (accessed 2021/03/04) , (Japanese Edition)

[15] The Tokyo Chamber of Commerce and Industry, "Results of the "Urgent Questionnaire on the Implementation Status of Telework" Survey", 2021, (Japanese Edition)

[16] H. Koyama, et al., "Risk Assessment of Telework for the New Normal Era", 2021 IEEE 10th Global Conference on Consumer Electronics, pp.573-574, 2021

[17] S. Tanimoto, et al., "Risk Assessment of BYOD: Bring Your Own Device", 2016 IEEE 5th Global Conference on Consumer Electronics, pp.511-514, 2016

[18] SCRIBD, "ISMS Risk Assessment Manual v1.4", https://www.scribd.com/document/202271054/ISMS-Risk-Assessment-Manual-v1-4, 2015

[19] H. Sato, et al., "Information Security Infrastructure", Kyoritsu Shuppan Co., Ltd., pp.29-32, 2010, (Japanese Edition)

[20] S. Tanimoto, et al., "A Study of Risk Assessment Quantification in Cloud Computing", 8th International Workshop on Advanced Distributed and Parallel Network Applications (ADPNA-2014), pp. 426-431, 2014

[21] S. Tanimoto, et al.," Risk Assessment Quantification of Ambient Service", ICDS 2015 : The Ninth International Conference on Digital Society, pp. 70-75, 2015