

February 12, 2021

To JICPA members

The Japanese Institute of Certified Public Accountants

Remote Work Series No.5

Remote Meetings and the Use of Remote Meeting Tools

Following the spread of novel coronavirus infectious disease (COVID-19), demand for new ways of living are growing, as well as new styles of working.

This environment has also led to an increase in opportunities for remote work using remote tools that had previously been used by some companies primarily for employees working from home, and as a meeting format, the use of remote meetings has also become common. On the other hand, there is also the risk that vulnerability of information security in the remote meeting tools themselves, or their incorrect use, could lead to leaks of the important information of the engagements in areas such as audit, taxation, and consulting.

Remote meeting tools themselves have the potential to allow certified public accountants (“CPAs”) to work more flexibly and efficiently, and by accurately understanding the risks associated with remote meetings and remote meeting tools, the probability to cause a major incident can be mitigated, and in the event of risks emerging, their impacts can be controlled.

The aims of this document are to understand the characteristics of remote meetings and using remote meeting tool, and then to summarize the situation primarily from the perspective of the risk of information leaks, so as to provide a reference that will contribute to the appropriate and efficient implementation of remote work by CPA offices including accounting firms (“CPA offices”).

<<I Basic approach>>

With companies and organizations increasingly implementing remote meetings, there has been a rise in requests from clients, etc. for CPA offices to respond accordingly. Given that it may become difficult to execute operations smoothly in cases where such requests are not met, and given the increased risk of infection that would result from an insistence on conducting only face-to-face meetings, it is desirable that organizations introduce some kind of remote meeting tool.

On the other hand, compared to the face-to-face meetings that have been held before, it is likely that the nature of such meetings will make it more difficult to limit the locations in which meetings take place, and the participants, and to ensure that the extent to which

materials are shared is appropriate. Given that the managements of CPA offices are required to understand the risk of information leaks, and to implement the necessary countermeasures, in a timely and appropriate fashion,¹ they should give due consideration to the fact that there are limits to the countermeasures to the risk that can be taken in relation to remote meetings and remote meeting tools, and decide policy accordingly.

When hosting the meeting it is especially important that careful consideration be given to how to deal with the event as an organization, because this involves such duties as the selection of remote meeting tools, monitoring, and attendee and materials management. Examples of such tactics include choosing a remote meeting tool that can only be used in participant mode, and establishing and enforcing rules during participation in meetings.

<<II Main risks associated with remote meetings and remote meeting tools>>


Category	Title/overview	Explanation of risk
Usage policy	No rules/regulations for meetings and meeting tools	In cases where there are no rules within the organization to handle new meeting formats or to determine whether or not the use of new meeting tools is permitted, there is a danger that users will deploy remote meeting tools without considering security issues, or not maintain security during meetings.
Uncovering remote meeting-related risks	Risks not uncovered, or not reviewed for long periods of time	Remote meeting-related risks are relatively new, and new risks themselves are being recognized frequently. Unless a PDCA cycle of extracting a list of specific remote meeting-related risks from a trustworthy organization such as Japan's Information-technology Promotion Agency, evaluating them and responding to them is not implemented at an appropriate frequency that takes into account the characteristics of each risk, there is a danger that risk awareness will become outdated.
Remote meeting tool-related risks	Risk associated with contracts (When hosting meetings)	Remote meeting tool services are provided by a variety of operators, but the reverse side of the ease of use offered by many of them is the danger of using a provider or vendor that is not bound by strict obligations with regard to confidentiality and unexpected data usage.
	No restrictions on remote meeting tools which can be used (For both host and participants)	In cases where the remote meeting tools that can be used have not been designated and restrictions have not been applied in advance, there is a risk that users will use remote meeting tools without permission that have not been subject to a security evaluation, or that do not conform to the organization's rules. It should be kept in mind that, especially when clients specify a remote meeting tool that has not been used before, there may be cases where it is difficult to give a clear response, making it impossible to avoid using the tool.

Refer to ¹IT Committee Research Report No. 4 "Guidelines for Information Security in CPA Engagements", IV 1.

	Operators have not taken countermeasures to address the vulnerability of remote meeting tools (For both host and participants)	There are remote meeting tools that are not (cannot be) updated for a certain period of time, despite vulnerability having emerged. Continued uses of such remote meeting tools leads to a heightened risk of information leaks.
	Monitoring is not performed to check whether the continued use of a remote meeting tool is permitted (When hosting meetings)	If timely or periodic checks are not made for changes in the service level or security condition after the use of a remote meeting tool has commenced, there is a heightened risk of remote meetings being conducted without an awareness that the security level is different from the level when the remote meeting tool first began to be used, leading to information leaks.
	Risk associated with termination of contract / suspension of use (For both host and participants)	There is a risk that no process exist to terminate a contract for services that do not conform with the internal rules of the CPA office (audit corporation), or a risk that the termination of contract or suspension of usage cannot be communicated to users in a timely fashion, resulting in the continued use of a service that does not satisfy security levels, etc.
Risks associated with implementing remote meetings	Existence of unexpected participants	There is a risk that unrelated individuals participate in the meeting as a result of the host having erroneously sent the meeting URL to organizations or people who were not originally intended to be invited, or due to the host or participants inadvertently sharing the meeting URL.
	Establishing an environment for meeting participation	In cases where it is difficult for the host to confirm the environment in which the participant attends the meeting, for example, when attending a remote meeting from home, this can lead to the risk of meeting contents being leaked to others living in the same dwelling, by making the meeting screen visible or the sound audible, or the risk of information leaks via a smart speaker.
	Participation using a public network	The risk of information leaks is heightened if no restrictions are put on the usage of unencrypted public Wi-Fi (such as hotel LANs, etc.) by participants.
	Unauthorized	There is a risk that participants use smartphones or tablets to take recordings of the meeting without

recording/pictures of the meeting taken by participants	permission from the host, or use snapshot functions to take pictures.
Unauthorized sharing or dissemination of recordings by the meeting host	In cases where the meeting is being recorded, there is a risk that the meeting host shares recorded data with persons other than the participants, without the participants' authorization. There is also a risk that the meeting host erroneously leaks or disseminates recorded data.
Risk of information being shared outside the meeting	When information is shared during the meeting with other participants, there is a risk of the sharing of information that should not have been shared. For example, displays of the desktop or folders can show what kind of information is being retained, or materials are projected on screen by mistake, or during the sharing of materials a pop-up appears on screen from a chat application or some other source.

<<III Examples of countermeasures>>



Leadership*

- ◆ Deciding/reviewing policy on remote work in general, including remote meeting-related issues
- ◆ Establishing and reviewing remote meeting-related rules
- ◆ Establishing and reviewing remote meeting-related risk assessments and policy on risk countermeasures
Keep in mind that the risk of remote meeting will vary depending on the confidentiality of the information being handled.
- ◆ Review contract template for remote meeting-related issues, consider revising existing contracts
Keep in mind the advisability of allocating tasks to individuals with the necessary skills in both legal and IT.
- ◆ Implement education and training with regard to remote meetings

*Indicates chief executive officers such as heads of firms or managing directors of CPA offices.



Person in charge of security

- ◆ Establishing and reviewing remote meeting-related risk assessments and policy on risk countermeasures
Keep in mind that the risk of remote meeting will vary depending on the confidentiality of the information being handled.
- ◆ Reviewing rules in relation to outsourcing, including those for remote meetings tools
- ◆ Select and conclude contracts for remote meeting tools that can be used, and consider additional measures
Keep in mind the need to deal with meetings where highly confidential information is handled and meetings where it is not, as well as differences between meeting hosts and participants.
- ◆ Gather information about the vulnerabilities of software used, including remote meeting tools
- ◆ Decide whether to allow upgrades to latest versions of remote meeting tools
- ◆ Make manuals available to explain what remote meeting tools can be used, and how to use them. Include which individual functions with security implications, within tools, can be used, and how to use them (subtitles, recording, backgrounds, etc.)
- ◆ Make remote meeting manuals available
In such cases, consider the following points.
 - Warnings related to the implementation environment when participating in a remote meeting from home, etc. (use a separate room, use earphones, turn off smart speaker functionality, etc.)
 - Confidentiality level, handling of recordings or recorded information, confirmation in advance regarding with whom information from material used is to be shared
 - Method for adding participating members
 - Method for sharing schedule data with others
 - Use of security code (connection ID) when entering meeting room
 - Set password for meeting
 - Use waiting room function (waiting area before the meeting room itself)
 - Confirm prohibition of unauthorized pictures or recordings when meeting starts
 - Use meeting lock
 - Measures for dealing with unintended information sharing (shut down unnecessary software, use background picture, do not share full screen, suspend chat pop-ups for the duration of the meeting, etc.)



User

- ◆ Performing engagements in accordance with the rules of CPA offices

<<IV Useful websites>>

1. IT Committee Research Report No. 4 “Guidelines for Information Security in CPA Engagements”

https://jicpa.or.jp/specialized_field/20201028ajf.html

2. Information-technology Promotion Agency (IPA)

- Security precautions for teleworking

<https://www.ipa.go.jp/security/announce/telework.html>

3. Ministry of Internal Affairs and Communications

- Ensuring security for teleworking

https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/

4. ICT Information Sharing and Analysis Center Japan

- Reference guide for working from home safely and comfortably

<https://www.ict-isac.jp/news/news20200701.html>