

品質管理基準報告書第1号周知文書第1号

2021年2月12日

会 員 各 位

日本公認会計士協会

リモートワーク対応第5号

リモート会議及びリモート会議ツールの活用に関する周知文書について

2021年2月12日

改正 2022年10月13日

日本公認会計士協会

監査・保証基準委員会

(周知文書：第1号)

新型コロナウイルス感染症の拡大により、新しい生活様式が要請され、働き方についても新しいスタイルが求められている。

そういった中で、従来から一部の企業や在宅勤務の方を中心に活用されていたリモートツールを用いたリモートワークの機会も増加し、会議形式としてもリモート会議が一般化してきている。一方でリモート会議ツール自体の情報セキュリティ上の脆弱性や、誤った利用によって、監査、税務、コンサルティング等の業務における重要な情報の流出につながってしまうリスクも存在する。

リモート会議ツール自体は公認会計士の働き方を柔軟にかつ効率的に変えていくことのできるものであり、リモート会議及びリモート会議ツールに対するリスクを正しく把握し対応していくことで、重大な事象を起こす蓋然性を軽減し、リスクが顕在化した場合にその影響を限定的にすることができる。

本周知文書は、リモート会議及びリモート会議ツール利用時（以下「リモート会議関連」という。）の特徴を理解の上、公認会計士事務所（監査法人）においてリモートワークを適切かつ効率的に実施することに資するための参考として、主に情報漏洩リスクの観点から取りまとめられたものである。

本周知文書は、一般に公正妥当と認められる監査の基準を構成するものではなく、会員が遵守すべき基準等にも該当しない。また、2021年2月12日時点の最新情報に基づいている。

《Ⅰ 基本的な考え方》

リモート会議を実施する企業・組織は増加しており、公認会計士事務所（監査法人）がクライアントなどから対応を求められる機会は増加してきた。対応しないことで、業務を円滑に遂行することが難しくなる可能性や、対面型でしか会議を行えないことで会議参加者の感染リスクが高まる可能性もあることから、組織として何らかのリモート会議ツールを導入することが望ましい状況にある。

一方、今まで実施してきた対面型の会議と比べ、その性質上、会議の実施場所や参加者を限定することや、資料の共有を適切な範囲で行うことが難しいと考えられる。公認会計士事務所（監査法人）の経営者は、情報漏洩のリスクの適時・適切な把握、必要となる対策の実施を行うことが求められることから¹、リモート会議及びリモート会議ツールに対するリスク対策に限界があることを考慮に入れ、方針を決めることになると考えられる。

特に会議の主催者になる場合、リモート会議ツールの選定・モニタリング・出席者管理・資料管理などを行う責務が伴うことから、組織として会議を主催する場合の対応については慎重に検討することが望ましい。参加者としてのみ利用可能なリモート会議ツールを選定したり、会議参加時のルールを作り徹底させたりすることはその一例である。

《Ⅱ リモート会議及びリモート会議ツールに対する主なリスク》

分類	タイトル/概要	リスクの説明
利用方針	会議や会議ルールの規程・ルールが存在しない	新しい会議形式への対応、新しいリモート会議ツールの採用可否など定めることができるルールが組織に無い場合、利用者がセキュリティを考慮せずリモート会議ツールを導入したり、会議時のセキュリティが保たれなかったりするおそれがある。
リモート会議関連のリスクの洗い出し	リスクが洗い出されていない、又は長期にわたり見直されていない	リモート会議関連のリスクは比較的新しく、また、新しいリスク自体も頻繁に認識されている。独立行政法人情報処理推進機構（IPA）などの信頼できる組織から具体的なリモート会議関連のリスクを抽出し、評価し、対応する PDCA サイクルを、そのリスク特性も踏まえて適切な頻度で実施しないとリスク認識が陳腐化するおそれがある。
リモート会議ツール関連リスク	契約に係るリスク （主催者の場合）	リモート会議ツールは様々な事業者によってサービスが提供されており、簡易に利用ができるものも多い反面、秘密保持や想定外のデータ利用に関して義務が強く課されていないプロバイダー・ベンダーを利用してしまうおそれがある。
	利用可能なリモ	利用可能なリモート会議ツールをあらかじめ指定・限定しない場合、セキュリティ評価が行われてなか

¹ 品質管理基準報告書第1号-IT委員会実務指針第1-4号「公認会計士業務における情報セキュリティの指針」IV 1. 参照

	<p>ート会議ツールを限定していない (主催者・参加者とも)</p>	<p>ったり、組織のルールに適合していなかったりするリモート会議ツールをユーザーが勝手に利用してしまうリスクがある。特にクライアントから利用したことのないリモート会議ツールを指定された場合、明確な回答が出来ないためやむを得ず使ってしまうケースに留意する。</p>
	<p>リモート会議ツールの脆弱性の対応が事業者によってなされない (主催者・参加者とも)</p>	<p>脆弱性が生じているにもかかわらず、一定の期間内に対応しない(出来ない) リモート会議ツールも存在する。このようなリモート会議ツールを利用し続けてしまうと、情報漏洩リスクが高まる。</p>
	<p>リモート会議ツールが利用可能であり続けることをモニタリングしない (主催者の場合)</p>	<p>一旦利用を開始したリモート会議ツールに対して、サービスレベルの変更やセキュリティの状況を適時、又は定期的に確認していないと、リモート会議ツール利用開始時と異なるセキュリティ水準であるにもかかわらず、それを意識しないまリモート会議が行われてしまうため、情報漏洩リスクが高まる。</p>
	<p>契約停止・利用中止に係るリスク (主催者・参加者とも)</p>	<p>公認会計士事務所(監査法人)内のルールに対応できないサービスに対して契約停止を行うプロセスがない、又は契約・利用停止を利用者に適時に伝えないことで、セキュリティ水準等に達していないサービスを受け続けてしまうリスクが存在する。</p>
リモート会議実施に関わるリスク	<p>想定外の参加者の存在</p>	<p>主催者が誤って本来参加しないはずの組織・人に会議 URL を送ってしまったたり、主催者・参加者が不用意に会議 URL を共有したりすることで無関係な人物が会議に参加してしまうリスクが生じる。</p>
	<p>会議参加環境の整備</p>	<p>主催者は参加者の会議参加環境が確認しづらく、例えば、家庭からリモート会議に参加する場合、会議画面が見えたり、音漏れによって同居者に会議内容が漏れたり、スマートスピーカーを通じて情報が漏洩するリスクが生じる。</p>
	<p>公共のネットワークを利用した環境からの参加</p>	<p>暗号化されていない公共 Wi-Fi (ホテルの LAN 環境など) を利用しての参加などを制約しないと情報漏洩リスクが高まる。</p>
	<p>会議参加者による会議の無断録画・撮影</p>	<p>会議参加者がスマートフォンやタブレットを使い主催者に無断で会議を録画したり、スナップショット機能を用いて撮影するリスクが存在する。</p>

	会議主催者による録画内容の無断共有及び拡散	会議を録画する場合、録画データを会議主催者が参加者に無断で会議参加者以外と共有してしまうリスクが存在する。また、会議主催者が録画データを誤って漏洩・拡散してしまうリスクも存在する。
	会議外の情報の共有リスク	会議時に他の参加者に情報を共有する際に、本来共有すべきでない情報を共有してしまうリスクが存在する。例えば、デスクトップやフォルダの表示により、どのような情報を保持しているかが見えてしまう、誤った資料を投影してしまう、共有中にチャットなど画面上のポップアップが表示されてしまう、などが考えられる。

《Ⅲ 対応策の例》



経営者※

- ◆ リモート会議関連を含むリモートワーク全般の方針の決定・見直し
- ◆ リモート会議関連規程の整備・見直し
- ◆ リモート会議関連のリスク評価とリスク対応方針の整備・見直し
その際、取り扱う情報の機密性によりリモート会議のリスクも異なることにも留意する。
- ◆ リモート会議関連についての契約雛型の見直し、既存契約の見直しの検討
その際、法務・IT両面で必要なスキルの有る担当を割り当てることに留意する。
- ◆ リモート会議に関する教育研修の実施

※公認会計士事務所（監査法人）における所長、理事長等の最高経営責任者等を指す。



セキュリティ担当者

- ◆ リモート会議関連のリスク評価とリスク対応方針の整備・見直し
その際、取り扱う情報の機密性によりリモート会議のリスクも異なることにも留意する。
- ◆ リモート会議ツールを含む外部委託に係る規程の見直し
- ◆ 利用可能リモート会議ツールの選定、契約、追加的な対応の検討。機密性の高い情報を扱うリモート会議とそうでない会議がある場合の対応、会議主催者と参加者による違いにも留意する。
- ◆ リモート会議ツールを含む利用ソフトウェアの脆弱性に関する情報収集
- ◆ リモート会議ツールの最新版への更新可否の決定
- ◆ リモート会議ツールの利用可否、使い方に関するマニュアルの整備。セキュリティにも関連するツール内の個別機能の利用可否と利用方法の整理も含む（字幕、録画、背景等）。
- ◆ リモート会議に係るマニュアル整備
その際に以下のような点を検討する。
 - 家庭等からリモート会議に参加する際の実施環境に係る注意（部屋を分ける、イヤホン着用、スマートスピーカーの機能を止める等）
 - 機密性レベル、録画及び録画情報の取扱い、利用資料の情報共有に係る相手先との事前確認
 - 参加メンバーの追加方法
 - 相手先とのスケジュールデータの共有方法
 - 会議室入室時のセキュリティコード（接続ID）の利用
 - 会議パスワードの設定
 - 待合室（会議室前室）機能の利用
 - 会議開始時の無断撮影・録画の禁止の確認
 - ミーティングロック利用
 - 意図しない情報共有対策（不要なソフトを終了する、背景画像の利用、全画面共有を行わない、チャットのポップアップの会議期間中の停止等）



利用者

- ◆ 公認会計士事務所（監査法人）のルールに則った業務の遂行

《Ⅳ 参考になるウェブサイト》

1. 品質管理基準報告書第1号-I-T委員会実務指針第1-4号「公認会計士業務における情報セキュリティの指針」

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

2. 独立行政法人 情報処理推進機構（IPA）

- ・ テレワークを行う際のセキュリティ上の注意事項

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

3. 総務省

- ・ テレワークにおけるセキュリティ確保

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

4. 一般社団法人 ICT-ISAC

- ・ 家庭内で安全快適に在宅勤務を行うためのリファレンスガイド

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

以 上

- ・ 本周知文書（2022 年 10 月 13 日改正）は、次の公表物の公表に伴う修正を反映している。
 - － 監査基準報告書（序）「監査基準報告書及び関連する公表物の体系及び用語」（2022 年 7 月 21 日改正）