『リモートワーク』における管理面からの留意点等

従前から働き方改革の一環として『リモートワーク』が推進されておりますが、新型コロナウィルス感染症の拡大により新しい生活様式が要請され、このところ一気に『リモートワーク』の機会が増えてきており、『オフィスワーク』という今まで労務管理や内部統制等の当り前の前提としてきたことが大きく変貌して、オフィス外での雇用主と従業員との間に物理的・心理的に距離のある環境を前提にする管理体制、手法が求められてきております。

クライアントの皆様からも、①如何に労働時間管理を行えばよいか、業績評価をどのように行うかという労務管理の視点や、②相互牽制を前提として構築される内部統制システムを如何に有効に整備し運用して行けばよいかという内部統制の視点、また③情報にかかるセキュリティ対策という視点からご相談を受けることが多くなっており、今回の GTM ニュース-会計実務-では『リモートワークにおける管理面からの留意点及び対策について』述べてみたいと思います。

1. リモートワーク下での労務管理について

① 労働時間管理はどのように行うか

リモートワークは企業側と従業員側とで物理的・心理的に距離感があることで「労働時間の管理が難しい」「仕事の評価がしづらい」という点に問題を感じる声が多い。

この点、労働時間の管理に関しては、労働基準法に従う必要があるが、厚生労働省は労働時間の適正な把握のために使用者が講ずべき措置を明らかにすべく「労働時間の適正な把握のための使用者が講ずべき措置に関するガイドライン」（平成 29 年 1 月 20 日策定）を策定していることから、当該ガイドラインを遵守してリモートワークを行う時の留意点を述べてみたい。

従来のオフィス内での勤務の場合、その勤務状態を確認可能な状態で、タイムカードや IC カードでの電子記録により時間の管理を行うことができたが、オフィス外である場合は、直接その勤務状態を確認できないため、パソコン等の起動時間により自動的に勤務時間を管理する等のシステム的な対応により確認することになる。しかし、そのようなシステム的な対応ができない企業では、従業員の「自己申告制」により勤怠管理システムに出社退社時間を登録することにより確認するケースも多いようである。

この自己申告制を採用して確認する場合、前述の「労働時間の適正な把握のための使用者が講ずべき措置に関するガイドライン」では下記の３点について留意すべきとされていることに留意しなければならない。

ⅰ）自己申告を行う労働者や、労働時間を管理する者に対しても自己申告制の適正な運用等ガイドラインに基づく措置等について、十分な説明を行うこと。

ⅱ）自己申告により把握した労働時間と、入退場記録やパソコンの使用時間等から把握した在社時間との間に著しい乖離がある場合には実態調査を実施し、所要の労働時間の補正をすること。

ⅲ）使用者は労働者が自己申告できる時間数の上限を設ける等適正な自己申告を阻害する措置を設けてはならないこと。さらに36協定の延長することができる時間数を超えて労働しているにもかかわらず、記録上これを守っているようにすることが、労働者等において慣習的に行われていないかについて確認すること、である。

現状のリモートワークでの労働環境において（急な対応としてリモートワークを実施している企業）は、「自己申告制」による労働時間管理が多くなっているようなので、労働時間管理が十分にできず労働基準法に抵触するリスクが高まってきていると考えられる。

上記ガイドラインに記載されている 3 点にご留意いただき、リモートワーク下における労働時間管理が適切に行われているかを改めてご確認いただきたい。

② 業績評価をどのように行うか

既述のように、リモートワークは企業側と従業員側とで物理的・心理的に距離感があるので、その業務の成果が見え辛く「仕事の評価をし辛い」という課題に直面する。

このような中で「目標管理」を行って、日々の業務の中で成果を上司と部下とで確認しあい、その達成状況に応じた評価を行うということが有効といわれている。この「目標管理制度」では、1 日の業務開始時の業務確認、業務終了後の成果確認を電話、電子メール、テレビ会議・Web 会議システム等を使用して行い、日々の業務の成果や進捗状況を上司が直接把握することによって、その成果を評価することで管理する手法である。

従来から「目標管理制度」においては、評価対象の「成果」を如何に明確に定義するかというが重要と言われているが、同じオフィスの中で簡単に声掛けをして状況確認できていた環境とは異なり、リモートワーク環境の中では、朝晩の定例的な Web 会議での進捗確認を行う等、上司にとってはより積極的に部下との接触の機会を設けないと、その成果を評価する情報が得られない。すなわち従来よりも上司がより積極的にコミュニケーションをとることが必要になっている点に留意する必要がある。

リモート環境下における業績評価で重要な点は、上司と部下とで明確な目標設定を行うということであり、その成果を Web 会議等によりその達成状況を適時に評価し、次のアクションプランについて合意するということである。これは管理マネジメントサイクルといわれる、いわゆる PDCA サイクルを回転させることに他ならない。リモートワーク環境においてこそ、この PDCA サイクルが適切に回せるだけの目標設定等の対応ができているかが重要であり、改めてご確認いただきたい。

2.　リモートワーク下での内部統制に関して

日本公認会計士協会は、企業側・監査人双方のリモートワークの動向に関連する課題・論点を検討して、論点整理を行い提言を取りまとめることを目的に、リモートワーク対応プロジェクトチームを組成し、リモートワーク対応第 1 号から第 5 号を以下のように公表している。

公表日	リモートワーク対応への提言
2020.12.25	電子的媒体又は経路による確認に関する監査上の留意事項 ～監査人のウェブサイトによる方式について～
2020.12.25	リモート棚卸立会の留意事項
2021. 2.12	PDF に変換された証憑の真実性に関する監査上の留意事項
2021. 2.12	構成単位等への往査が制限される場合の留意事項
2021. 2.12	リモート会議及びリモート会議ツールの活用について

これらの内容は、企業側の検討論点としては「①業務プロセス・内部統制の見直しに係る課題の整理、②電子的情報の真正性担保の仕組みのための調査研究」を目的としており、監査人側の検討論点としては「①電子的監査証拠の利用の促進及び課題の整理、②監査報告書の電子化に係る課題の整理、③残高確認電子化に係る実務上の課題の整理、④情報セキュリティに係る提言」を目的としている。

特に企業側の検討論点である、「①業務プロセス・内部統制の見直しに係る課題の整理」では、証憑が紙から PDF に移行することに伴って、PDF 変換プロセスに係る内部統制を新たに構築しなければならないことについての留意事項が取り纏められているのでご確認いただきたい。

すなわち、リモートワークが導入される以前から、紙媒体の証憑を PDF 変換して証跡としてサーバーに保管したり、シェアードサービス会社に PDF 変換したデータを送って情報システムに入力又は照合を行っている会社もあるが、PDF の真正性を担保するような内部統制の構築がより一層重要となるということである。具体的には、PDF への変換時において、故意又は不注意により『PDF と原本の不一致が生じていないことを確かめる統制の検討』や、故意による改竄は PDF への変換前と変換後のそれぞれの段階で行われる可能性があることに留意し、『改竄を発見・防止する仕組み（例えば電子署名）を検討』する必要があるということである。

また、電子媒体の証憑を PC のディスプレイ上で目視照合する場合、紙媒体の証憑をチェックマークを付けながら手作業で照合するよりも精度が低下する可能性がある。サブディスプレイを配布する会社もあるが、『役席者の検印（電子承認を含む）があれば良いというものではなく、役席者がどのような検証を行った上での検印であるかの方が重要』であり、これは「オフィスワーク」も「テレワーク」でも変わるところではないため、実効性のある内部統制を構築する必要があることに留意を要する。

なお、監査人側の検討論点とされる項目についても、首都圏からの往査が困難な状況下において内部監査（モニタリング）を実施する上でも参考になる情報でもあるので、監査人側の論点についてもご参照いただきたい。

リモートワークが内部統制に与える影響については、今後も GTM ニュース-会計実務で取り上げる予定である。

3.　リモートワークにおけるセキュリティ管理について

「オフィスワーク」から「リモートワーク」への移行（作業場所が「オフィス」から「自宅」へ）により、必然的にネットワーク環境も「オフィス」から「自宅」に移行することになる。すなわち、堅牢な社内イントラネットではなく、「自宅」のインターネットを利用することから個人所有の情報機器のセキュリティが重要になる。具体的には、家庭内のルーターのセキュリティ設定、WiFiのセキュリティ設定を見直す必要があるが、これらはセキュリティポリシーによるルール化だけでは不十分である。従業員がルールを遵守するためには情報セキュリティに係るリスクと必要性を理解（腹落ち）する必要があり、そのためにはセキュリティに関する教育研修が重要となる。

また、厳重な施錠管理、入出管理が行われているオフィスでの「オフィスワーク」であればPC自体の紛失・窃盗のリスクが問題となることはあまりないが、「リモートワーク」では各家庭のホームセキュリティに依存するため、貸与PC自体が紛失・窃盗した場合であっても情報漏洩の実害を発生させないための方策を講じる必要がある。（ハードディスク全体の暗号化等）

さらに、「オフィスワーク」から「リモートワーク」への移行は、勤務状況が見えづらくなるという特徴から「オフィスワーク」では社内の目がありできなかった外部記憶媒体（USBメモリー等）の利用よるデータの流出、個人PCの業務利用等に対しても「リモートワーク」では容易になるというリスクもある。（USBメモリーの利用をシステムで制限）

どのような堅牢なセキュリティを構築したとしても利用者が無効化するリスクがあるため、セキュリティ対策はハード面の強化だけでなくソフト面（教育研修）も併せて実施する必要がある。

なお以下にリモートワーク上のセキュリティ対策を考える際に参考となる Web サイトを記載したのでご参照いただきたい。

●総務省
　テレワークセキュリティガイドライン
https://www.soumu.go.jp/main_sosiki/cybersecurity/telework/
●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
●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

以上