

## 働き方解説(第2回)

### テレワーク導入時の課題や対策について解説

2021.03.15



2020年以降、急速に導入が進むテレワークは新しい働き方として注目されていますが、導入の際にはテレワークの課題や問題点についても知っておく必要があります。この記事では、テレワークの課題や問題点と併せて、それらの解決策を解説します。加えて、テレワークの現状についても見ていきましょう。

#### テレワークの現状について

もともと、テレワークやリモートワークといったオフィス外で仕事をする働き方は昔から存在していました。日本でテレワークの導入が本格化したのは、2019年の働き方改革関連法の施行のタイミングです。従来の働き方にとらわれず、柔軟な働き方で労働者の労働環境の改善と生産性の効率化が主な目的になっていたといえるでしょう。

そんな中、2020年に世界中で爆発的に流行した新型コロナウイルスの登場によって、感染症対策としてテレワークを導入する企業も増えました。結果としては、新型コロナウイルスの存在がテレワークの普及に最も影響を与えたといえるでしょう。

その結果、日本でも多くの企業がテレワークを導入しました。都内企業のテレワークの導入率の調査結果を見ると、2018年には19.2%でしたが2019年には25.1%、2020年には51.4%にまで普及が進んでいます(「テレワーク導入率調査結果」2021年1月東京都調べより)。

2021年1月時点ではテレワーク導入率は57.1%となっており、今後もさらに導入企業は増えていくことでしょう。

#### テレワークの課題や問題点



先ほどの都内企業のテレワーク導入率の推移を見ると、2020年4月には62.7%まで上昇したもののその後50%ほどまで下がっています。その理由として、テレワークの課題や問題点が明らかになったのも原因の1つと考えられます。テレワークにはどのような課題や問題点があるのか、1つずつ見ていきましょう。

#### 〈勤怠管理が煩雑〉

テレワークは大きく分けると在宅勤務・モバイルワーク・サテライトオフィスと働く場所によって種類が異なります。しかし、いずれも社外で働くものであり、勤怠管理が煩雑になってしまいがちです。従業員の長時間労働や働きぶりをチェックできない点で、勤怠管理が煩雑になるという課題が挙げられます。

#### 〈セキュリティリスク〉

テレワークでは社外で仕事をするようになるため、情報漏えいや不正アクセスなどのセキュリティリスクが高まります。テレワーク用のデバイスの紛失・盗難による情報漏えいや、社内ネットワークに接続するためのVPNのID・パスワードが漏れて不正アクセスにつながる、などのリスクが考えられます。

#### 〈コミュニケーション不足〉

従来は同じオフィス内で直接会話ができましたが、テレワークではそれが行えません。テレワークにおける主なコミュニケーション手段はテキストを使ったメールやチャットになるため、コミュニケーション不足に陥る可能性があります。コミュニケーションが不足すると、上司から部下への指示が的確に伝わらなかったり、情報の行き違いで業務効率が低下したりすることが課題として挙げられます。

#### 〈導入コストがかかる〉

テレワークを実施するには、環境を構築しなければなりません。VPNやリモートデスクトップツールの導入だけでなく、テレワーク用のデバイスやWi-Fi環境の準備などにもコストがかかります。テレワークによってオフィスにかかるコストや従業員の異動コストを削減できる半面、導入時のコストがかかる点も課題の1つです。

#### 〈仕事の評価がしづらい〉

コミュニケーション不足の課題と通じるものとして、従業員の仕事の評価がしづらい点も課題として挙げられます。上司が部下の仕事の評価しようにも、離れた場所で仕事をしているため誰がどのタスクに対応しているかの把握が煩雑になり、評価がしづらくなります。従来通りの評価基準ではテレワークに則していない可能性が高く、評価基準の見直しも必要になります。

テレワークの課題の解決策を解説



これらのテレワークの課題・問題点について、具体的にどのような対策を行えばよいのでしょうか。ここでは、課題の解決策について解説します。

#### 〈社員へセキュリティ対策の教育を行う〉

セキュリティリスクが高まる課題に対しては、社員へセキュリティ対策の教育を行うことが解決策となります。テレワークは、オフィス外のため、監視の目が行き届きにくくなります。最終的なセキュリティ事故の発生有無は、従業員のセキュリティリテラシーに委ねられます。

こうした背景から、テレワークの実施におけるルールを策定し、その中でセキュリティ対策を盛り込んで周知徹底させなくてはなりません。もちろん、人への対策だけでなく、体系的な対策も行うことが重要です。最終的には人の行動によってセキュリティ事故の発生有無は変わってくるため、人に対する対策をサポートする意味合いで体系的な対策を施すとよいでしょう。

#### 〈タスク管理ツールを導入する〉

タスク管理ツールはプロジェクトの進行を可視化して、分かりやすく管理するツールです。誰がどのタスクを対応しているか、進捗具合はどの程度か、などを関係者全員で共有し、業務を効率的に進められます。

テレワークではコミュニケーションが不足しがちです。おのおののタスクや進捗具合を可視化することは非常に重要です。管理者側も部下の仕事ぶりをチェックできれば、テレワークにおけるコミュニケーション不足や仕事の評価がしづらい、といった課題の解決策となり得ます。

#### 〈情報通信サービスの導入〉

先ほどのタスク管理ツールのように、情報通信サービスやツールの導入で、テレワークにおける課題や問題点の多くは解決できます。例えば、勤怠管理も勤怠管理システムを導入すれば、遠隔地でも管理は可能です。その他にも、コミュニケーション不足の解決策として、ビジネスチャットツールやビデオ会議ツール、グループウェアなども考えられるでしょう。

現在では非常に多くの情報通信サービス・ツールが存在し、「こんなものがあつたらいいな」と思うようなものはほとんど存在しています。テレワークを導入する際の自社の課題を明確にして、課題を解決できる情報通信サービスの導入を検討しましょう。

#### 〈ファイルストレージサービスの利用〉

ファイルストレージサービスは、オンラインストレージやクラウドストレージなどとも呼ばれるサービスです。インターネットに接

続いていけば利用できるサービスであり、必要なファイルを複数人で共有するのも可能です。

テレワークにおけるセキュリティリスクの対策として、業務に必要なファイルをファイルストレージサービスに格納することも解決策として考えられます。ファイルを手元のデバイスに保存しなければ、情報漏えいのリスクもありません。

ファイルストレージサービスはアクセス制限も可能であり、サービス事業者がセキュリティ対策を施しているため不正アクセスの心配もほとんどないといつてよいでしょう。

## まとめ

テレワークは昔から存在していますが、日本では2019年に施行された働き方改革や、2020年に流行した新型コロナウイルスの影響で急速に普及しました。21年1月時点では、都内企業の約半数以上がテレワークを導入している状況です。

しかし、テレワークには、勤怠管理が煩雑になることやセキュリティリスク、コミュニケーション不足などの課題・問題点が存在しています。それらの課題・問題点に関しては、情報通信サービスの導入などの解決策が有効です。テレワーク導入の際の参考にしてみてはいかがでしょうか。

※掲載している情報は、記事執筆時点のものです