基本のキ。セキュリティ入門（第8回）

リモートワークの導入で変わるオフィスの在り方

2021.01.04

近年、働き方のトレンドが大きく変わりつつあります。厚生労働省が推進している働き方改革や、2020年の新型コロナウイルスの影響により、リモートワークの普及が急速に進みました。リモートワークの普及によって、現在のオフィスの在り方はどのように変わるのでしょうか。

この記事では、リモートワークによる働き方の変化から、今後のオフィスの在り方、リモートワークで想定されるトラブルの例をご紹介します。

オフィスには行かない？昨今のリモートワークの導入で変化する働き方

「仕事は出社してオフィスで」という考え方が変化しています。リモートワークを導入し、自宅やカフェなど、特定のオフィス以外で仕事ができる環境が整備されつつあるのです。

＜リモートワークを導入する企業が増加＞
リモートワークは新型コロナウイルスの影響で一気に普及が進みました。東京都が2020年6月に調査した結果によれば、都内企業のリモートワーク導入率は57.8％で、2019年の25.1％と比べて2.3倍にも上昇しています。

この調査は従業員30人以上の都内企業約2000社の回答によるもので、企業規模に関係なくリモートワークの導入が進んでいるのが分かります。

さらに、リモートワークの継続を考える企業は80.4％で、そのうち40.6％はリモートワークの拡大も視野に入れています（東京都「テレワーク導入実態調査結果」より）。今後もリモートワークの広がりが予想されるでしょう。

＜昨今の働き方のトレンド＞

働き方のトレンドは、リモートワークを活用した形態に移行しているといえます。そもそもリモートワークとは、ICT（情報通信技術）を利用して時間や場所にとらわれない多様な就労形態を表します。勤務先のオフィスから遠く離れた自宅やカフェ、レンタルオフィス、コワーキングスペースなどでも、ICTを利用することで新しい働き方を実現できます。

なお、リモートワークと似た言葉としてテレワークがありますが、意味はほとんど同じです。

リモートワークの導入により変わるオフィスの需要と在り方

リモートワークの導入によって、働き方だけでなくオフィスの在り方も変わりつつあるのをご存じでしょうか。都内企業の中にはオフィスを不要と考える企業もあり、オフィスがなくなることによって新たなメリットも生まれています。

＜リモートワーク導入で都心のオフィスを解約する企業も＞

リモートワークを導入したことで、主にITベンチャーで都心の本社オフィスを解約する企業が出てきました。人材育成を動画で支援する企業やマッチングサービスを展開する企業、スタートアップを支援する企業などは全面的にリモートワークに移行し、オフィスを解約したり縮小・移転したりしています。

理由として、リモートワークでも従来通り働けることや、従業員の心理的なメリットが挙げられています。

＜リモートワークによるコスト削減について＞

都心にオフィスを構えると、膨大なコストを固定で払い続けることになります。例えば、駅に近いビジネスエリアにオフィスを構える場合、賃料や光熱費で毎月数百万円のコストが発生します。

リモートワークが導入できればオフィスの必要性が低くなり、固定でかかるコストが削減できます。加えて、オフィス内で利用するコピー機や紙などの備品も節約でき、大幅なコスト削減が可能です。

オフィスの縮小・解約をする前に確認！リモートワークのよくあるトラブル例

リモートワーク導入でオフィスは不要になりつつありますが、リモートワークでの働き方を進めていくとトラブルが発生するケースもあります。これからご紹介するトラブル例を把握したうえで、リモートワークの実施やオフィスの縮小・解約を検討しましょう。

＜端末の紛失、盗難による情報漏えい＞

リモートワークでは社外で仕事をするため、ノートパソコンなどのモバイル端末を利用します。その際に注意すべきは端末の紛失・盗難です。社内データを端末に保存したまま紛失・盗難の被害にあうと、情報漏えいのセキュリティ事故につながる可能性があります。

実際にあったトラブルとして、リモートワーク用の端末を移動中の電車内で紛失した事例があります。この事例では端末上に顧客データを保存した状態で紛失したため、データを盗み見られて取引先にセールスの電話が来るようになり、苦情が寄せられるトラブルに発展しました。

端末の紛失・盗難による情報漏えいは自社の信頼低下にもつながるため、注意が必要です。

＜不正侵入、不正アクセス＞
リモートワークでは社外から社内ネットワークへの通信経路を用意するため、ネットワークのセキュリティ対策がしっかりと行われていないと、外部からの不正侵入、不正アクセスのリスクが高まります。

また、システム的な対策が行われていても、ネットワークにアクセスするためのIDやパスワードが第三者の目に触れやすい状態だったり、別のサービスと同じパスワードを使い回していたりすると、悪用される可能性が高くなります。従業員一人ひとりのセキュリティ意識を向上させる必要もあるでしょう。

＜マルウエア感染＞
リモートワークにおいて気を付けるべきセキュリティトラブルとして、マルウエアへの感染も挙げられます。ウイルスを含む不正なソフトウエアの総称であるマルウエアは、常に機密情報を狙っていると考えて対策を講じましょう。

リモートワークではVPNなどを利用して社内ネットワークに接続しますが、端末がマルウエアに感染してしまうと、社内ネットワーク全体に被害が及ぶ可能性があります。

マルウエア感染を防ぐには、リモートワークで利用する端末へのアンチマルウエアソフトの導入はもちろん、利用できるソフトウエアを限定して従業員に周知徹底することが重要です。

＜データの消失＞
リモートワークを実施する際にはデータの消失にも注意しましょう。リモートワーク実現のためにクラウド上にデータを保存して利用する機会も増え、大切なデータが消失してしまう可能性も考えられます。

実際に2020年11月には公益財団法人ふくい産業支援センターが運営する「ふくいナビ」でクラウドサーバー上のデータが消失した事例がありました。

データ復元を専門とするアドバンスドテクノロジーでは、リモートワークにおけるデータ消失の問い合わせ増の事態を受けて注意を促しています。クラウドやローカル環境内だけにデータを保存するのではなく、複数環境でデータをバックアップしておくことが重要です。

リモートワーク化のお困りには！NTT西日本の「フレッツ・SDx」

東京都内では2020年のリモートワークの普及率が前年比で2.3倍にも上昇し、働き方やオフィスの在り方にも変化が訪れています。オフィスを不要と考える企業も登場し、オフィスの解約による大幅なコスト削減などもリモートワークを導入する大きなメリットになっています。

ただし、リモートワーク時には端末の紛失・盗難による情報漏えいや、マルウエア感染などのトラブル例も報告されており、導入の際にはしっかりとした事前準備が欠かせません。

また、急きょリモートワークを導入した企業の中には、ネットワークの混雑が原因で通信速度が低下し、思うように業務が進められない企業も存在します。

リモートワークの導入を検討されている方の中には、こんな悩みをお持ちの方もいらっしゃるのではないでしょうか。

・拠点間の通信を遅延することなく、スムーズに実現したい
・OSのアップデート時期は通信が遅くなり、業務に支障が出る
・人材不足の影響で拠点の通信ネットワークの管理、設定まで手が回らない

NTT西日本では、低遅延・高セキュリティなVPN通信を実現する「フレッツ・SDx」を提供しています。フレッツ・SDxはインターネットを介さない閉域網のIP-VPNであるため高セキュリティであり、フレッツ

光ネクストを利用した高速通信で映像データなどの大容量データも低遅延でリアルタイムに通信可能です。

さらに、遠隔操作可能なコントローラーを通じて各拠点の機器を自動で設定でき、ネットワーク管理も効率的に行えます。働き方改革や新型コロナウイルスの影響によるリモートワークの実現が迫られる今、対応にお困りの方はお気軽にご相談ください。

※掲載している情報は、記事執筆時点のものです