APO-社会保険労務士法人
第 124 号
発行日　2018.7.1

APO-社労士通信

テレワークの活用

最近社会の様々な場面において、「テレワーク」の活用が進んでいます。「テレワーク」とは、「テレ＝離れたところで」と「ワーク＝働く」を組み合わせた造語で、主として情報通信技術（ICT＝Information and Communication Technology）を活用した、場所や時間にとらわれない柔軟な働き方をいい、働く場所によって、在宅勤務、モバイルワーク、サテライトオフィス勤務の 3 つの形態の総称として使用されています。今回は、厚生労働省策定の「情報通信技術を利用した事業場外勤務（テレワーク）の適切な導入及び実施のためのガイドライン」に沿って、主なポイントをご案内します。

■テレワークのメリットとデメリット

通常の事業場での勤務と比べて、テレワークには労使双方に以下のようなメリットがあります。

◆労働者にとってのメリット…通勤時間の短縮、業務の効率化･時間外労働の削減、育児や介護と仕事の両立の一助になる、仕事と生活の調和を図ることが可能 等

◆使用者にとってのメリット…業務効率化による生産性の向上、育児･介護等による労働者の離職の防止、遠隔地の優秀な人材の確保、オフィスコストの削減、非常時の事業継続性（BCP の確保）等

一方で労働時間の管理や仕事と仕事以外の切り分けが難しく、長時間労働になりやすい、情報漏洩の危険性がある等の課題があります。

■労働基準関係法令の適用と留意点

通常の労働者と同様に、テレワークを行う労働者にも、労働基準法、最低賃金法、労働安全衛生法、労働者災害補償保険法等の労働基準関係法令が適用されますので、制度導入時には以下についての対応が必要となります。

（１）労働基準法の適用に関する留意点…テレワークを行う場所等の労働条件の明示を行い、以下の取扱い等について労使間でルールを定めて、労働時間の適正な管理を行う必要があります。

① いわゆる「中抜け時間」について （休憩時間や時間単位の年次有給休暇として取扱うことが可能）

② 通勤時間や出張旅行中の移動時間中のテレワークについて（使用者の明示、または黙示の指揮命令下で行われるものは労働時間に該当）

③ 勤務時間の一部でテレワークを行う際の移動時間等について（使用者の指揮命令下に置かれている時間であるか否かにより、個別具体的に労働時間に該当するか休憩時間に該当するか判断をする）

（２）長時間労働対策…メール送付時間の抑制や、休日・深夜のシステムへのアクセス制御等により、長時間労働による健康障害防止を図ることが求められます。

（３）労働安全衛生法の適用に関する留意点…健康診断、長時間労働者に対する医師による面接指導、及びストレスチェックについて、その結果等を受けた措置の健康確保措置を講じる必要があります。

（４）労働災害補償の適用に関する留意点…テレワークにおける災害は、私的行為等の業務以外が原因であるものを除き、原則として業務上の災害として労災保険給付の対象となることを労働者に十分周知することが望まれます。

■テレワークの導入と実施の留意点

上記の法令の適用における留意点の他にも、実際に導入する際には以下の点にも注意が必要です。

（１）労使双方の認識の確認、（２）業務の円滑な遂行方法の明確な提示、（３）業績評価等の取扱いの明確な提示、（４）通信費、情報通信機器等のテレワークに要する費用負担の取扱いの明確化、（５）社内教育等の取扱いの充実化

また労働者においても、勤務する時間帯や自らの健康に十分に注意を払い、作業能率を勘案して自律的な業務の遂行が求められます。テレワークは多くの課題があるものの、今後いっそう普及することで、より創造的な能力を効率的に発揮し得る社会の実現が期待されます。

知っておきたいミニ知識　テレワークセキュリティ対策

多くの場合、企業の「情報資産」はオフィスの中で管理され、外部の目に触れることはありませんが、テレワークを行う場合は、インターネット上を流れ、持ち運びが容易なノートパソコン等の端末で利用されます。そのためインターネットを経由した攻撃を防御する対策がなされたオフィスとは異なり、ウイルスの感染や、記録媒体の紛失・盗難、通信内容の盗聴等の「脅威」にさらされやすいといえます。このとき、端末の設定や使い方に脅威に対する脆弱性が存在すると、情報漏洩や情報消失等の実際の事故に繋がります。企業が情報セキュリティを効率的に行うには、保護すべき情報資産を洗い出し、どのような脅威や脆弱性、リスクがあるのかを把握、認識した上で、重要度に応じた情報のレベル分けを行い、さらにレベル分けに応じた体系的な対策を実施することが重要です。

このとき、情報セキュリティ対策には「最も弱いところが全体のセキュリティレベルになる」という特徴があります。どこか１箇所に弱点があれば、他の対策をいくら強化しても全体のセキュリティレベルの向上には繋がりません。情報資産を守るためには、「ルール」「人」「技術」の三位一体のバランスがとれた対策を実施し、全体のレベルを落とさないようにすることがポイントとなります。

また、実際にテレワークで行う作業内容や予算によって、「テレワーク端末への電子データの保存の有無」「オフィス端末との関係」「クラウドサービスの利用の有無」を踏まえて検討し、経営者・システム管理者・テレワーク勤務者それぞれの立場からテレワークセキュリティの保全に関して正しい運用を認識する必要があります。

総務省のテレワークセキュリティガイドラインには、多くの日本企業で採用されている情報セキュリティ対策をベースとした、「経営者向け」「システム管理者向け」のそれぞれについて基本的な考え方が記載されていますので、参考の上、継続的に安全を確保していくため、企業・組織にあった対策を検討していきましょう。

ECOVIS®
お問い合わせは下記までご連絡ください。
APO-社会保険労務士法人　〒162-0824 東京都新宿区揚場町 1-18 飯田橋ビル 7F
Tel：03(5228)1990　sic.info@apol.jp　http://www.apoutsoucing.jp