はじめに

テレワークの導入を検討する場合、大きく、①勤務形態の変更に伴う規程等のルールの見直しと、②組織外でPC等の端末を利用することに伴うシステムやセキュリティ対策の導入の、2つの点を考慮する必要があります。2020年4月に、改正新型インフルエンザ等対策特別措置法に基づく「緊急事態宣言」が発令された際には、社内規程等の見直し・修正を行う十分な時間がなく、緊急避難的にテレワークを導入した企業もあったと思われます。

ただし、テレワークと言っても、勤務場所を自宅や居所とする在宅勤務を指す場合や、企業の組織外で仕事をする場合（モバイルワーク）、企業が契約しているシェアオフィスのような場所（サテライトオフィス）で仕事をする場合も含めるかによって、規程の見直し・修正の範囲や導入する対策は異なってきます。

最近では、新型コロナウイルス対策の長期化への懸念や働き方改革も見据え、勤務形態を見直す動きも活発になってきています。とるべき勤務形態の変更や対応の方法については、表1に示す国のガイドライン等を参考に、検討することをお奨めします。

表1　テレワーク導入時に参考にすべきガイドライン等

資料名	発行元	発行年月
テレワークセキュリティガイドライン（第4版）	総務省	2018年4月
テレワークを実施する際にセキュリティ上留意すべき点について	内閣サイバーセキュリティセンター（NISC）	2020年4月
テレワークモデル就業規則～作成の手引き～	厚生労働省	2017年3月
情報機器作業における労働衛生管理のためのガイドライン	厚生労働省	2019年7月
情報通信技術を利用した事業場外勤務の適切な導入及び実施のためのガイドライン	厚生労働省	2019年9月
第20回テレワーク推進賞～働く人が幸せになる社会へ～ 事例集	一般社団法人日本テレワーク協会	2020年2月

社内規程等のルールの見直し

テレワークの導入に際しては、勤務形態の変更にあたるため、就業規則等の社内規程の見直し・修正が必要になることには触れましたが、労働時間管理をどのように実施するかも検討が必要です。

すでにタイムカードが電子化されている場合は、そのままの対応で済みますが、物理的なカード等を用いて労働時間管理を行っている企業は、PCの使用記録から管理する方法や上司や役職者にメールで報告をする仕組みなど、ルールを決めておくとよいでしょう。

加えて、テレワークを導入すると、管理が及ばないところでの従業員の長時間労働が発生するリスクや、ハラスメント（セクハラ、パワハラ）のリスクも指摘されていますので、その点の対策も必要でしょう。

PC等の企業貸与の機器を社外に持ち出すにことについては、秘密保持に関して、「テレワーク宣誓書（仮称）」といった資料を差し入れてもらう対応も重要です。また、テレワークの導入前に、セキュリティや情報管理の留意点について、研修（e-learning）を実施することも検討しておきたいところです。

派遣社員のテレワーク実施に関しては、派遣先の企業内で働くことを前提として、勤務場所や時間、システムの使用（例として社外メールが発信できないなど）に関して、派遣先企業の従業員とは異なる条件を設けている場合があります。こうした前提を確認するとともに、派遣先と派遣元との合意に従って対応する必要があります。新型コロナウイルスの影響から、派遣契約を打ち切らざるを得ない事情が発生した場合でも、労働者派遣法の規定に従った適切な対応が求められます。

テレワーク導入時のセキュリティ対策

テレワーク導入時のセキュリティ対策としては、大きく、①情報の持ち出しの問題と②会社システムへの接続に関する問題が考えられます。

まず、情報の持ち出しについては行わない方が安全ではあるのですが、やむを得ず持ち出しをする場合でも、紛失のリスクを避けるため、紙での持ち出しは最小限にしたいところです。紙資料を持ち出す場合には、管理台帳で誰が、いつ、どの情報を持ち出したかを記録すると同時に、原本ではなく、コピーを取って持ち出すなどの対策が必要です。

紙資料をスキャンしてPDF化することで、紙資料の削減を進めていたおかげで、新型コロナウイルスの影響下でもスムーズにテレワークが実現できたという事例もあります。

資料や情報が会社貸与のPCに入っていてそのまま持ち出す場合も、持ち出した情報が何かを特定できるよう、管理台帳を作成しておくことは重要です。PCに不正にアクセスされたり、紛失したりする場合に備え、データの暗号化対策も必要になります。USBなど外部接続装置の使用は禁止されている場合が多いですが、端末の持ち帰りを許可する場合には、そうした対策がしっかり効いているかを確認することも重要です。

情報を会社のサーバーに転送する場合には、ネットワーク経路の安全性を確保するために、**VPN**（Virtual Private Network、仮想的な専用線でつなぎ、盗聴リスク等を避ける仕組み）を利用しましょう。テレワーク時の作業場所の物理的なセキュリティは、企業と同じというわけにはいきませんが、ネットワーク面においてはVPNを使用することで、作業環境によるセキュリティ強度の差を低減することができます。

スマートフォンに関しては、紛失や盗難に備えて、**モバイルデバイス管理（MDM）**のツールを導入している場合もあると思います。万一、紛失や盗難に遭った場合に、端末を初期化してくれる機能があるものなどは安心ですが、セキュリティを重視するあまり、従業員のプライバシー保護を軽視しないよう、注意が必要です（端末の位置情報の設定をオンにする場合など）。

会社のシステムへの接続については、会社貸与のPCを使うか個人のPCを使用する（**BYOD**、Bring Your Own Device）かで対応が変わってきます。

会社貸与のPCの場合、社内にいる場合とほぼ同じ操作が可能となる方法で会社のシステムへ接続するよう、設定を行うことが考えられます。また、シンクライアント [1] であれば、多くの情報が端末側に残らないため、セキュリティ面でも安心です。

注意しなければいけないのは、接続に際し、信頼できるネットワークを使っているかどうかです。無料のWi-Fiなどは、暗号化されていなかったり、強固ではない暗号化方式が使われていたりすることがありますので、そうしたネットワークからの社内ネットワークへの接続は許可しないなどの対策が必要になります。

個人のPCを使用する場合もいくつかの方式がありますが、OSのバージョンや導入しているウイルス対策ソフトなどによっては、会社のシステムへの接続が制限される場合もあります。

リモートデスクトップと呼ばれる方式は、会社貸与のPCだけでなく、個人のPCでも利用可能なため、テレワークの適用範囲を拡大できるメリットが考えられます。事前にアプリケーションをダウンロードしておくか、専用のUSBキーをPCに差し込んで使用する方法などがあります。セキュリティ上はなりすましに注意が必要なため、通常のID／パスワードに加え、生体認証なども用いた多要素認証の導入を行うことが多いでしょう。

テレワークを導入する場合には、この他にクラウドサービスを利用することもあります。会社内での作業自体が、クラウドサービスを利用することを許可していることが前提になりますが、設定のミスから情報漏えいやデータ消去といったリスクにつながるケースもあることには、注意が必要です。

従業員1人ひとりにおける留意点

テレワークでは、これまで解説してきた対策に加え、従業員1人ひとりが留意すべき点もありますので、ここでまとめておきます。

在宅勤務の場合、企業と同じとはいかないものの、ある程度の物理的セキュリティが確保されていますが、専用の仕事部屋などを利用しないケースでは、家族に情報を見られることもあります。スクリーンロックの実施、のぞき見防止フィルターの使用は有効と考えます。
また前述した、USBなどの外部接続装置の使用無効化や、家族との端末の共用を避けるなどの対策も必要です。

加えて、テレワークでは画面が小さく目が疲れるという意見も聞きます。セキュリティ対策そのものではありませんが、大型モニターの使用をサポートしたり、VDT（Visual Display Terminals）作業の時間を管理したりするなどのケアも、業務上のミスを防ぐという意味で有用でしょう。

まとめ

新型コロナウイルス感染防止対策を期に、一気に導入が加速したテレワークですが、今後も働き方改革やワークライフバランス向上の観点から、この動きは継続するものと考えられます。緊急事態宣言の発令時には、緊急避難的にテレワークを導入した企業においても、社内規程等のルールの整備とセキュリティ対策の導入によって、多様な働き方をサポートできるように取り組んでいって欲しいと思います。

次回は、「**テレワークを導入・実施するうえで注意すべきサイバーセキュリティリスクと攻撃手法**」および本稿での説明を踏まえ、セキュリティ対策にかかるコストについての考え方を解説します。

最後に、この記事を執筆するにあたり、以下の書籍を参考としました。