テレワーク実施にあたっての セキュリティ上の注意点

新型コロナウイルス感染症の影響により、引き続き自宅で業務を行うテレワークが推進されている。IPA（＝独立行政法人情報処理推進機構）が発表した「テレワークを行う際のセキュリティ上の注意事項」と、内閣サイバーセキュリティセンターによる「テレワーク等への継続的な取り組みに際してセキュリティ上留意すべき点について」を基に、テレワークを行う上でのセキュリティ上の注意点を紹介する。

テレワーク環境の有無で注意事項が変わる

新型コロナウイルス感染症（COVID-19）の影響により、ITを用いて自宅でも業務が行えるような環境を整えて、社員等を出社させずに事業継続を図る動きが急速に進んでいる。所属組織から支給されたパソコンを用いて、通常勤務と同じ利用環境（テレワーク環境）を実現する方法もあれば、一方で、そのような環境が提供されない状況もあるため、双方のケースにおける注意事項を紹介する。

所属先が定めた規程やルールをよく理解して、従うことが重要

まず、所属する組織や企業からテレワーク環境が提供されている場合、テレワーク勤務者は、使用するテレワーク環境に関して所属先が定めた規程やルールをよく理解し、それに従うことが大切だろう。またシステム管理者は、テレワークを行う従業員にパソコン等端末を支給する場合は、組織外への持ち出しに係る管理等が円滑かつ適切に進められていたかについて確認することが重要になる。また、関連するOSやソフトウェアのアップデート等必要な脆弱性対策が実施されていたか、外部からのサイバー攻撃を受けた形跡はないか等の確認も必要となる。適宜、手続きや対策の見直しを行うことや、支給台数が業務量に十分に対応していない場合等には、支給端末の追加導入の検討を行うべきである。

次に、所属する組織や企業からテレワーク環境が提供されておらず、自宅のパソコン等で業務に関わるメールの送受信や資料作成等を行う場合には、セキュリティ対策を強く意識したい。支給外端末の利用に関しては、システム管理者等に、利用状況や必要に応じた例外措置等の手続きの実施について確認することも重要となり、支給端末を使用する場合と同様に、関連するOSやソフトウェアのアップデート等、必要な脆弱性対策が実施されていたか、外部からのサイバー攻撃を受けた形跡はないか等について確認することも必要だ。ITにそれほど詳しくない、相談できるシステム管理者がいない等の状況にある場合は、普段使っている個人の環境のセキュリティ対策を見直すことから始めたい。

個人の意識も高めて積極的にセキュリティ対策を

テレワークを行う際は、各自でセキュリティ対策を行う

ことも重要になる。使用するパソコンやソフトウェアで用いるパスワードは複雑にし、多要素認証が利用できる場合は、是非活用しよう。また、端末や機器は最新の状態にアップデートして、セキュリティの穴をふさいでおきたい。不審なメールには特に注意が必要で、添付ファイルは開かないように注意。文面に記載されたリンクは偽サイトの可能性があるので、不用意にクリックしたり、IDやパスワードを入力しないようにすべきである。

公共の場所で作業を行う場合は、情報漏洩のリスクが高まるのでVPN（Virtual Private Network）接続の機能などを活用して通信路を暗号化する。また、他者からの盗み見（ショルダーハッキング）や大声での電話会議による盗聴のリスクにも注意。公共の無線LAN（Wi-Fi）はセキュリティ設定が甘かったり、偽の無線LANの可能性もあるので利用する際は十分注意する必要がある。持ち運びしやすいノートパソコンやスマートフォン、USBメモリ等は盗難、紛失のリスクもあるので、万が一に備えてデータを暗号化しておくと安心だ。

テレワークの実施にともない利用が拡大している遠隔会議システムは、外部ネットワークを使うこととなるため、組織での導入・運用状況及び外部委託先や外部の組織・個人が提供する遠隔会議システムの利用状況について確認し、必要なセキュリティ対応が実施されているかについて確認することが欠かせない。また、遠隔会議システムにおいて、どのような情報の取り扱いまで利用可能とするかを含め、安全性を確保しつつ、有効活用を行うために、必要なポリシーを整備しておきたい。

テレワーク中は、どんなに警戒していてもいつ何が起こるかわからない。インシデント発生時に備えて連絡方法を事前に確認しておき、インシデントに気づいたら迷わず迅速に対応することが重要である。

職場に戻る際も気を抜いてはいけない

テレワークから職場に戻る際にも注意点がある。まず、所属する組織や企業からテレワーク環境が提供されている場合、職場のパソコンを持ち帰って仕事をしていた人は、職場のネットワークに繋げる前にOSやアプリのアップデート、セキュリティソフト定義ファイルのアップデート、パソコン内のウイルスチェックなど、所属先が定めた規程やルールをよく理解して、それに従うこと。

次に、所属する組織や企業からテレワーク環境が提供されていない場合、自宅のパソコン等で業務を実施していた人は、パソコンに保存されている業務ファイルやメール等について、所属先の環境への受け渡し方法や自宅のパソコンの業務ファイルの削除方法を確認。USBメモリを使用する場合は、個人情報の保存、持ち出し、暗号化、ウイルスチェック等について、同様に所属先の規定やルールに従い、持ち運ぶ場合は紛失しないように細心の注意を払いたい。