中小企業のセキュリティー対策

―37―

テレワークの導入には

基本的な対策の徹底を

東京商工会議所が8日に公表した「新型コロナウイルス感染症への対応に関するアンケート」によると、テレワークを実施している企業は26・0％、実施検討中は19・5％であった。また、現在テレワークを実施していない企業では、「テレワーク可能な業務がない」場合を除き、「社内体制の整備」「パソコンなどハードの整備」「セキュリティー確保」を課題として挙げている。テレワークの実施には課題はあるが、感染症対策の一つの手段として検討したい。

「セキュリティー確保」に関して、テレワーク時は普段と異なる業務環境となるため特別な注意も必要となるが、まずは基本的な対策を徹底してほしい。独立行政法人情報処理推進機構（IPA）では基本的な対策として、次に掲げる「情報セキュリティ5か条」の実践を推奨している。

①OSやソフトウエアは常に最新の状態にしよう！
②ウイルス対策ソフトを導入しよう！
③パスワードを強化しよう！
④設定を見直そう！
⑤脅威や攻撃の手口を知ろう！

例えば、テレワークに使用する端末が私有端末の場合、ウイルス対策ソフトを必ず導入し、OSやソフトウエアが最新になっていることを確認してから業務を行う。会社支給の端末であっても、管理者によるソフトウエアなどの更新管理ができないようにするため、ワンタイムパスワードなどの二要素認証の設定がある場合は利用する。設定がない場合は、パスワードは英数字記号含め10文字以上に設定して使い回さないことが重要である。ファイル共有にOSの共有設定やクラウドサービスを利用している場合は、共有範囲を改めて確認してほしい。

さらに、緊急時は情報などをだまし取ろうとするサイバー攻撃が増加する傾向がある。IPAでは、1月に新型コロナウイルスを題材としたウイルス付きメールを確認している。最近ではSNSやショートメッセージを悪用して偽サイトに誘導する攻撃も報告されている。セキュリティー関係機関やベンダーの注意喚起などを注視していただきたい。

注意したい4項目

基本的な対策のほかに、次に掲げる項目にも注意してほしい。

■情報管理

社外へ持ち出してよい情報か確認し、不必要な持ち出しや私有端末に保存しないなど情報のレベル分けに応じた管理を行う。

■物理管理

会社から持ち出した書類や端末、外部記憶装置などは盗難・紛失しないよう安全に管理し、持ち運ぶ場合は暗号化などの対策を施す。また、第三者が多く集まる場所では書類や端末の画面をのぞき見られないように注意する。

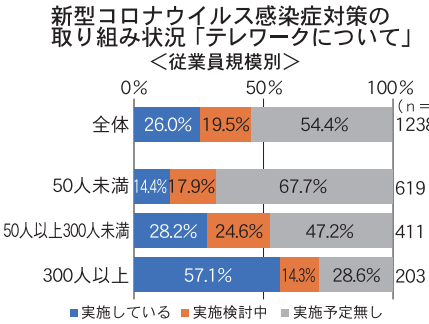
■無線LAN利用

無線LANを利用する場合は、通信を暗号化して盗聴対策を行う。また、攻撃者が情報窃取のために仕掛けた偽Wi―Fiスポットも存在するので、信頼できるものだけ利用する。

■外部サービス利用

ファイル共有やメッセージングサービスなどの外部サービスで会社指定以外のものを利用する場合、セキュリティー上の問題がないか管理者に相談する。

テレワークの実施に向けて情報セキュリティー対策を検討する場合は、IPAが発行する「中小企業の情報セキュリティ対策ガイドライン」（QRコードを参照）を参考にしてほしい。



出典：東京商工会議所「会員企業の防災対策に関するアンケート付帯調査　新型コロナウイルス感染症への対応について」

（独立行政法人情報処理推進機構・江島将和）