

中小企業のテレワークとセキュリティ管理

テレワークは「Tele＝離れた所」と「Work＝働く」の造語で、導入することにより時間や場所にとられない柔軟な働き方が可能となる。雇用労働者が行うテレワークは①在宅勤務（自宅で業務を行うテレワーク）、②モバイルワーク（営業活動等により外出先で業務を行うテレワーク）、③サテライトオフィス勤務（本来の勤務先以外のオフィスで行うテレワーク）の3形態に分けられる。この違いは基本的に勤務場所の違いであるが、①③はフルタイム勤務が前提で、②より社内情報アクセスが制限されないことが望ましい。

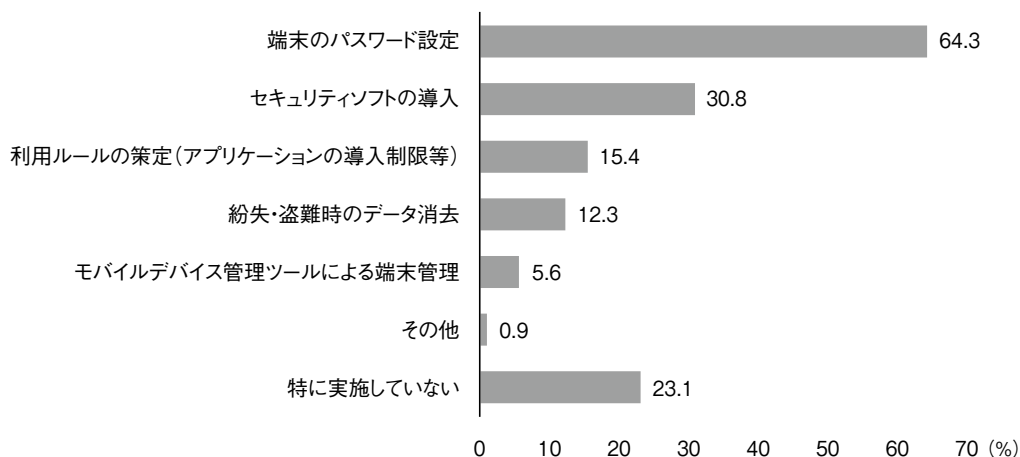
総務省「平成30年通信利用動向調査」によると、テレワークを導入している企業の割合は19.1%、導入予定がある企業の割合は7.2%であった。導入率はこれまで緩やかに上昇していたが、新型コロナウイルス感染拡大に伴い企業のテレワークへの関心は高まっており、導入の加速が予想される。

上記調査で企業が導入もしくは導入予定のテレワーク形態は②のモバイルワークが63.5%と最も多く、①の在宅勤務は37.5%、③のサテライトオフィス勤務は11.1%である。フルタイムでないオフィス外勤務形態であるモバイルワークは制度対応等において導入のハードルが比較的低く、中小企業にとって当面は②の導入が中心になると思われる。

モバイルワークで労働者が使用する端末はタブレットないしスマートフォンである。情報処理推進機構の調査によると、2016年度で40.0%の中小企業がタブレット端末及びスマートフォンを利用している。利用企業のうち、社員の私物端末の業務利用を認める企業は39.0%あり、小規模企業では46.7%と半数近い。タブレット端末及びスマートフォンへのセキュリティ対策は「端末のパスワード設定」を64.3%の企業が実施しているものの、「セキュリティソフトの導入」は30.8%、「利用ルールの策定（アプリケーションの導入制限等）」が15.4%など十分ではなく、「特に実施していない」も23.1%ある。

テレワークは働き方改革推進のうえでも、BCP推進のうえでも有効な手段だがセキュリティ対応を疎かにすると逆に企業の存立を脅かしかねない。テレワーク導入にあたっては、ハードウェアの整備や制度設計に加え、セキュリティ対策の充実が強く望まれる。（商工総合研究所主任研究員 江口政宏）

中小企業のタブレット端末やスマートフォンへのセキュリティ対策（複数回答）



（資料）情報処理推進機構「2016年度 中小企業における情報セキュリティ対策の実態調査」