視点を変えて可能性を広げるITの新活用術（第7回）

セキュリティリスクを「見える化」。情報流出を防げ

2023.06.20

コロナ禍を経て多くの企業でテレワーク、リモートワークが浸透した。現在は出社と在宅を組み合わせたハイブリッドワークを進める企業もあり、多様な働き方が広がっている。一方、情報管理の面でさまざまな課題も浮き彫りになっている。出社が当たり前だった時は部門の上司や同僚、IT担当者などがパソコン操作や情報の取り扱いについて相談に乗ったり、目配せしたりすることができた。だが、テレワークや社外で仕事をする機会が増える中、情報管理がおろそかになり、情報漏えいなどセキュリティリスクが高まっているのだ。

本人任せのパソコン管理がセキュリティリスクになる

従業員の働く意欲や人材確保などの観点からも柔軟かつ多様な働き方への取り組みが求められる中、改めて情報管理のあり方を考える必要がある。テレワークでは会社支給のパソコンであっても、その管理は本人任せになりがちだ。会社で仕事をしていればオンライン環境が前提になるのでパソコンのセキュリティパッチやウイルス対策ソフトの定義ファイルの更新なども自動的に実施したり、分からないことがあったりすればIT部門やヘルプデスクの担当者がサポートしてくれる。

だが、テレワークや社外で仕事をする場合、オフライン中はセキュリティベンダーがゼロデイ攻撃などに備えて配布するウイルス対策ソフトの更新は困難だ。加えて、従業員のITリテラシーなどの低さがセキュリティリスクを引き起こすこともある。例えば、Webサイト閲覧にかかわるリスクだ。勤務中に業務とは関係のないWebサイトの閲覧は従業員の生産性を低下させるだけでなく、意図せずに悪意のあるWebサイトにアクセスし、ウイルス感染して情報が盗まれるリスクもある。

情報流出のリスクがある外部メモリー… 続きを読む