ＳＯＭＰＯ未来研究所 主任研究員　内田 真穂氏

デジタル時代のリスクと保険（4）

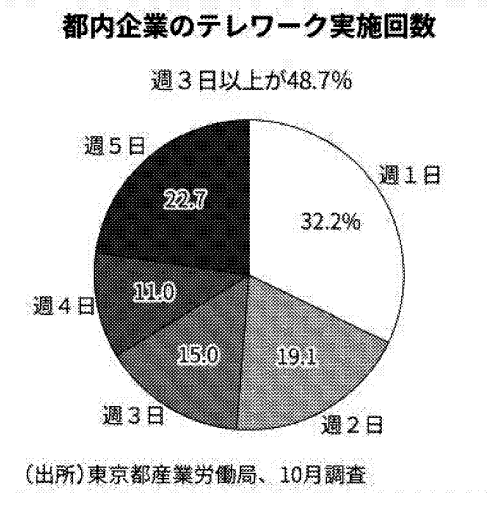
# テレワークに忍び寄る危機

この１年半余りでテレワークが一気に普及した。東京都の発表によると、2021年10月時点の従業員30人以上の都内企業のテレワーク実施率は55.4%。テレワーク実施回数は週３日以上が48.7%となっている。今後、新型コロナウイルス禍が収束しても、テレワークは主要な働き方の一つとして定着化しそうだ。そこで重要になってくるのがテレワーク環境におけるセキュリティーである。

これまで多くの企業では、企業ネットワークと外部ネットワークの境界にファイアウオールなどのセキュリティーを設置し、外部からの侵入を阻止してきた。

しかし、テレワーク環境はその境界の外に存在する。企業支給のパソコンを使用していても、適切なセキュリティー対策がなされていない自宅やサテライトオフィスのネットワークを利用することで攻撃対象となりやすい。私物パソコンを使用している場合には企業の管理が及ばないため、セキュリティーリスクがさらに高まる。

実際、テレワーク環境を狙ったサイバー攻撃が相次いでいる。例えば、仮想の専用ネットワーク（ＶＰＮ）などテレワーク用に導入している製品の脆弱性が悪用され、社内システムに不正アクセスされる、パソコンの業務情報などを窃取されるといった被害が発生している。セキュリティー更新プログラムを適用していないＶＰＮはたびたび攻撃に見舞われている。また、テレワークの普及とともに利用が拡大したウェブ会議ツールの脆弱性を突いて、ウェブ会議ののぞき見も行われている。




さらに、テレワーク環境下で増加傾向にあるのがフィッシング詐欺である。フィッシング詐欺とは実在する組織をかたってメールを送信し、個人情報を詐取する行為を言う。メールを使って偽サイトに誘導し、そこで個人情報を入力させる手口が一般的である。フィッシング詐欺対策の業界団体であるフィッシング対策協議会によれば、１回目の緊急事態宣言が出された20年４月と比較して、21年３月はフィッシング詐欺の報告件数が約４倍に増加した。

メールを使った犯罪ではビジネスメール詐欺（ＢＥＣ）も要注意だ。これは取引先になりすまし普段やり取りしている業務メールを装って偽の請求書や振込先変更依頼のメールを送ったり、経営幹部になりすまして偽の送金指示メールを部下に送ったりするもので、犯罪者の口座を送金先に指定して金銭をだまし取る手口である。

テレワーク環境下を狙った攻撃には、従業員の情報リテラシーの強化が欠かせない。システム対策については、総務省の「テレワークセキュリティガイドライン」や「中小企業等担当者向けテレワークセキュリティの手引き」が参考になる。

国内損保各社はテレワーク中の情報漏洩や会社支給パソコンの破損・盗難リスクなどを補償する「テレワーク保険」を販売している。ただ、ＢＥＣについては、経路こそメールだが、人の錯誤で金銭を振り込んだ損害であり、国内の通常のサイバー保険では補償対象とならない。海外ではＢＥＣ被害が一部補償される保険がある。

テレワーク環境を狙った攻撃は今後も増加し、ますます巧妙化していくと予想される。企業は自衛策を強める必要がある。

掲載日 2021年11月29日 日経産業新聞 018ページ