サイバーセキュリティ最前線

在宅勤務が急増している今こそサイバーセキュリティに万全を期すべきだ

新型コロナウイルスの感染拡大により、多くの企業が在宅勤務を奨励している。だが、その際に気になるのが在宅勤務時のセキュリティ対策だ。いかにオフィスでのセキュリティ対策を万全にしていても、在宅勤務時の対策がおろそかになっていては元も子もない。そこで、今号では在宅勤務時のサイバーセキュリティ対策について紹介したい。

新型コロナウイルスの感染拡大で、在宅勤務者が急増している。しかし、在宅勤務にはセキュリティに関して、多くの落とし穴があることに注意しなければならない。とくにここ数年はサイバー犯罪が急増しているので要注意だ。事実、全国の警察が昨年1年間に摘発した不正アクセスなどのサイバー犯罪は9542件（前年比502件増）、昨年1年間に検知したサイバー攻撃とみられる不審な通信は1日平均4192件（前年比52・3パーセント）と、どちらも過去最多となっている。そこで、今号ではセキュリティ会社である㈱ブロード（東京都千代田区）に在宅勤務時のサイバーセキュリティのリスクと対策について解説してもらった。

ブロードがまず懸念するのが、データの不正な流出の危険性だ。「通常、社外からはアクセス許可を出さないデータにも、アクセス許可を与えざるを得ないといった状況も考えられる。こうした情報の流出や漏洩のリスクに注意を払わなければならない」という。

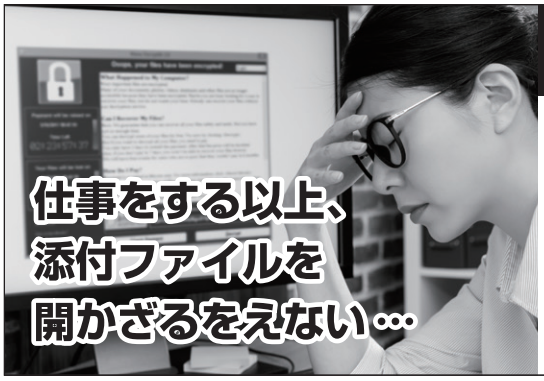
では、在宅勤務時にはどのような情報流出のリスクがあるのか。そのひとつが詐欺メールなどを契機とした情報流出である。「普段から『不審なメールは開かないように』といった具合に注意勧告がなされていると思うが、在宅勤務で周囲に相談できる相手がいないため、ついつい開けてしまう恐れがある」という。つねに正しいとはかぎらないヒトの判断に依存する方法は在宅勤務にかぎらずやめるべきだが、個々で仕事をする環境ではなおさらだ。

さらに業務でLINEをはじめとしたSNSやメッセンジャーツールを使用している場合も要注意だ。実際、LINEは2月26日に約4000人の利用者が不正ログインの被害を受けたことを発表。フィッシング詐欺などに使われる不正サイトへの誘導などが確認されたという。メールにかぎらずLINEなどを経由したフィッシングによっても、マルウェアが動作して企業情報を吸い取られてしまう恐れがあるので十分に注意を払わなければならない。

それから、セキュリティシステムが通常の勤務環境と同レベルで機能しているかという問題もある。この点について、ブロードは「企業・組織のネットワーク内で通信を監視・制御する仕組みの場合、それが在宅勤務時においても機能するかが重要になることが第一、ついで旧来型のセキュリティウイルス対策ではパターンファイルの更新や各パソコンの状態を管理者が把握するなどの課題もあり、こうした仕組みに依存しない対策が必要」とアドバイスする。

また、セキュリティにかぎらずトラブルが生じることはある。そういったときには在宅勤務時であっても技術担当者やセキュリティ担当者が早期に状態を把握できる体制をつくっておく必要がある。「事前に誰がどのように『ヘルプデスク』としての役割を担い、リモート操作などで問題解決にあたるかといったことをシミュレーションしておいてほしい。ただ、安直なリモート操作のツールの使用は、通信の安全性に疑問があったり、リモート操作が記録されず、監査できなくなったり、といったケースがあるので、こうした側面も含めて十分に検証してほしい」と。

新型コロナウイルスの感染拡大を機に、ともすれば在宅勤務の流れが加速する可能性もある。だが、そうなった場合にはますますここで紹介したようなリスクが増大することを忘れてはならない。ICT（情報通信技術）の発展でリモートワークは多様な形態で実現可能だが、先進的なセキュリティ対策でICTのメリットを安全に享受したい。



ウイルスを完全隔離※
添付ファイルを開く時の不安はこれで解消!!
従来とは全く異なる発想のセキュリティツール

Br Bromium®
［ブロミアム］

米国連邦政府機関をはじめ
世界と日本の重要な公的機関・有名企業を含む
400社以上がBromiumを導入しています

※2013年以降、Bromiumは推計20億以上のMicroVMが実行されましたが、侵害報告件数はゼロです。（米国Bromium社調べ）
詳細は［BROAD Security Square］で https://bs-square.jp/columbus

株式会社ブロード
〒100-0014 東京都千代田区永田町1-11-30 サウスヒル永田町7F
TEL：03-6205-7463（代表）