2020 年 10 月

マンスリー・ハイライト　拝啓社長殿

マネジメントのための経営財務情報

今回のテーマ：　サイバーセキュリティ

増加するサイバー攻撃

新型コロナウイルス対策によりテレワークの導入が拡大する中、テレワークを狙ったサイバー攻撃が増加しています。一般社団法人 JPSERT コーディネーションセンター公表の「インシデント報告対応レポート」[1]によると、同センターに寄せられたセキュリティインシデントの報告件数は、以下のとおり急激に増加しています。

【2020 年インシデント報告件数の推移※】

	1 月	2 月	3 月	4 月	5 月	6 月	7 月	8 月	9 月
件数	1,788	1,775	2,947	3,105	3,256	4,055	4,034	4,324	5,473

テレワークは、オフィス内で業務を実施することと異なり、社内システムへ外部からアクセスし業務を実施することになります。テレワーク下におけるサイバー攻撃では、遠隔から社内ネットワーク上のパソコンを操作する技術である「リモートデスクトップ」や、インターネット等のネットワークを通じてファイルを共有するクラウドシステムのサーバーなどを標的とするケースが多く報告されています。

テレワークにおけるサイバーセキュリティ

テレワークにおけるサイバーセキュリティ対策は、自社で実施しているテレワークの方式を確認・特定するところから始まります。総務省が公表している「テレワークセキュリティの手引き（2020 年 9 月 11 日）」[2]では、テレワークの方式を①テレワークで利用する端末種別、② オフィスへの接続方式、③ テレワーク端末へのデータ保存の有無、などにより、8 つに類型化し、考慮すべきセキュリティ対策が体系化されており参考になります。

「ルール」と「ひと」と「技術」のバランス

サイバーセキュリティ対策は、テレワークで使用するパソコン等の機器の設定や通信経路に関する「技術」に関する事項が中心となりがちです。しかし、テレワークはオフィスとは異なる環境で業務を行うことになるため、そのセキュリティ確保のための「ルール」を定めることから始める必要があります。加えて、それらを利用する従業員「ひと」の知識と意識を向上させることも重要です。セキュリティ確保に関する「ルール」をその目的から従業員が理解し、セキュリティに関する正しい知識を習得することが、不審なメールを開封しない、適切なパスワードを設定する等セキュリティ対策の基本事項の徹底につながります。

お見逃しなく！

サイバーセキュリティは「防御」という事前の対策に加え、従業員のパソコンがマルウェアに感染した、社内のサーバーが攻撃され情報が漏洩した等、実際にセキュリティ事故が発生したときに、迅速な対応策がとれるような体制を構築することも重要です。すなわち「事後」の対策です。体制の構築にあたっては、セキュリティ事故発生時を想定した演習を実施し、技術的な側面に加え、顧客への対応や広報等、幅広く検討することが有効です。

[1] https://www.jpcert.or.jp/pr/2020/IR_Report20201015.pdf

[2] https://www.soumu.go.jp/main_content/000706649.pdf