通信　i・ストリーム（法人版）VOL.43

文：小川 康成
ファイナンシャル・プランナー

愛知銀行と中京銀行の合併がニュースとなりましたが、長引く政策的低金利で銀行というビジネスモデル自体が毀損し、岐路に立たされているのかも知れません。

さて、今回は「新しい時代の新たな危険」について考えてみたいと思います。

新たな時代のニューリスク「サイバーリスク」について

今年は１年延期になった東京オリンピックが開催され、私も空手の中継にくぎ付けでした。組手競技では残念ながら金メダルを逃しましたが、「型」では喜友名諒選手が見事金メダルを獲得し、初開催競技の「空手」での金メダルに感慨深いものを感じました。

オリンピック期間中は世界中から日本に注目が集まりましたが、実は集まるのは注目だけではなく、オリンピック開催国は世界中のハッカー集団から攻撃を受けやすい。という事実もあり、中小企業者として、今までにないサイバーセキュリティを意識するべき時代に入ってきています。

中小企業の100%でサイバー攻撃を観測　（2018年の調査）

2019年に発表された神戸大学×大阪商工会議所×東京海上日動社の共同研究によると、商工会議所会員の中小企業の１００％でウイルス付メールや、不正なサイトへのリンクが添付されたメールも含め、悪意あるネット上の攻撃が確認されました。

また**約２割**の企業のパソコンから、**情報を見られたり、暗号化された情報が見られる状態**になっていた。外部からの遠隔操作が可能な状態になっている等、サイバー攻撃の被害にあっていた、もしくは遭う可能性が高い状態になっていたそうです。

同調査では、被害企業のうち約４分の１の企業から、メールを装ったウイルスメール攻撃などで、取引先の企業がサイバー攻撃を受け、それらが自社にも及んだそうです。

上記のような驚くべき実態調査が明らかになり、また年々攻撃の数は増えていて、一時期猛威を振るった「エモテッド」と呼ばれるマルウェアが再拡大しています。企業のパソコンが感染すると、自社のメールを装い、取引先にもウイルスメールを勝手に送信し始めるので、気が付いた時には元請け企業など取引先企業にも多大なる迷惑をかけ、場合によっては以後の取引停止という事態も考えられる程の脅威です。

- ◆ 取引先とメールでのやり取りはしていませんか？
- ◆ 社内のパソコンで外部のインターネットに自由に接続可能な状態になっていませんか？
- ◆ Wi-Fi（特にフリーWi-Fi等）を使用して、社用のパソコンを使用していませんか？

↑上記に一つでも当てはまるようであれば、注意が必要です。

個人情報保護法　令和４年４月１日に改正施行

そもそも個人情報とは何でしょう？

個人情報保護委員会の説明によれば、個人情報とは、「**生きている個人**に関する情報であって、その人が誰なのかわかる情報」をいいます。

例えば、「氏名」や「その人が誰なのかわかる映像」などが個人情報です。また、「携帯電話番号」や「住所」だけでは「その人が誰なのかわかる」とは判断できませんが、「氏名と住所」など、**他の情報と組み合わせることで「その人が誰なのかわかる」ようであれば、個人情報**です。

なお、公的な番号として１人に１つ、異なる番号が割り当てられた「マイナンバー」、パスポート番号や、指紋など個人の生体情報をデータ化したものも、それだけで「その人が誰なのかわかる」ので、個人識別符号と呼ばれる個人情報です。

令和４年４月１日の改正施行で、下記が変更となりました。

- 個人情報の漏えいが発覚した場合の**本人への通知が義務付け。**同様に※**委員会**への報告も必要。
- 委員会の命令違反の罰則が従来の 50 万円以下の罰金から、**１億円以下の罰金**へ引き上げ
- 情報の利用停止・消去等の個人請求権が法令違反の場合に加えて、正当な権利や利益が侵害

※　**個人情報保護委員会**

本人への通知が義務付けられた事により、お詫びの対応が増える事が予測されます。
もちろんですが、**従業員の情報も個人情報であり、社内での管理に注意が必要**です。

サイバー攻撃の重大性に政府も対応を開始

今年５月には米国最大の石油パイプラインが攻撃を受け、一時的に業務停止になりました。日本政府も重要インフラ事業者（金融機関、情報通信、電力、鉄道など）にサイバー防衛を義務付ける「重要インフラ行動計画」を明記し、企業へのサイバー防衛を義務付ける動きです。

サイバー攻撃でなくてもシステムが動かない金融機関がありますが、システムの脆弱性を突こうと真っ先に狙われないか？と心配になります。

同様に今後大手企業よりサプライチェーン（供給網）の安全確保を目的に、発注先の下請け企業にも、サイバー対策や意識向上を求める動きが広がる事も考えられます。

サイバー対策がウイルス対策ソフトだけ。という場合は、**“従業員がメールや添付ファイルを開いてしまう”**といった人が介在するサイバー攻撃に対応できないので、日頃からの訓練や意識向上の学習会などが有効です。

万一、サイバー攻撃被害に遭ってしまった場合は、**原因究明のために PC の点検などで、１台あたり 100 万円～200 万円と多額の費用が掛かります。**

ただ、どれだけ対策しても 100%の防御は難しいので、ウイルス対策ソフトの導入と合わせ、**サイバー被害を受けた際に補償対象となる保険**などに加入して、緊急時の多額な費用を補うのも良いでしょう。保険料は、意外とお安く数万円～加入可能です。

大手企業や取引先などからサイバー対策についての義務付けや確認が有った場合、きちんと回答出来るよう、自社の対策について考えてみる機会にして下さい。

Insurance agency
i・ストリーム

〒489-0976　瀬戸市井戸金町 422-1
電話(0561) 83-8111　　FAX(0561) 83-8131
ﾎｰﾑﾍﾟｰｼﾞ　http://istream-web.jp
E-Mail　istream@istream-web.jp