通信　i・ストリーム（法人版）VOL. 55

文：小川 康成
ファイナンシャル・プランナー

ロシアのウクライナ侵攻から１年が過ぎます。国連の安全保障理事会の常任理事国が、他国に対して易々と進行を仕掛ける事に驚きましたし、それだけではなく、現代の戦争らしく戦争前後でウクライナと支援国に対して、多数のサイバー攻撃が仕掛けられたという事実も出てきて、武力だけではない攻撃に対する備えも必要であることが証明されました。防衛力強化に向けた増税という話も出ましたが、日本の自衛隊サイバー部隊は約 500～800 人・予算 920 億円と他国に比べ非常に少ないようです。他国はどうかと言えば米軍が約 6,000 人で予算も１兆５千億円以上、中国は３万人規模、北朝鮮が 6,800 人となっており、一概に人数だけが能力とは言えないでしょうが、「量（数）は質に変化する」と言われるように多人数がいるから層が厚くなり能力の向上が高くなるのもあるでしょう。その意味で今回、開戦前のサイバー攻撃が失敗したといわれているロシア軍のサーバー部隊は約 1,000 人と言われており、自衛隊と大差がありません。

サイバー攻撃　民間企業も被害が増加

ロシアの侵攻に伴い、日本国内でのサイバー攻撃の検知数も 2021 年度比 29%増加と年々攻撃数自体が増えています。あるセキュリティ会社の調査では、**サイバー攻撃の数で日本は全体の８％を占め、米国に次いで２位でした。**国際的な位置づけを考えると重要な情報が集まる米国が狙われるのは当然ともいえますが、ほかの主要国を抑えて日本がワースト２位と言うのは意図的に狙われているのではと考えられます。攻撃は企業規模に関係なく行われており、大企業は目立つのでニュースになりますが、**中小企業の方がむしろセキュリティの甘さに付けこまれて実際に被害に会う確率が高いと言えます。**

大阪商工会議所の調べで、中小企業の約９割が調査で何らかのサイバー攻撃にさらされていた事がわかっております。昨年、愛知ではトヨタ系列の企業で、２月に**小島プレス工業が子会社経由の攻撃でトヨタ全工場が停止に追い込まれ**、３月には**デンソーが身代金を要求する「ランサムウェア」の感染で、トヨタ自動車の部品会社がサイバー攻撃を受けシステムに影響して 14 の工場の稼働停止**となり、被害が相次ぎ大きな話題となりました。その他にも、ブリジストン、パナソニック、月桂冠、しまむら、農協、安江病院など様々な分野でサイバー被害が報告されました。

メールやサイトから感染してパソコンを操作不能にして解除して欲しければ身代金を払えと要求する**「ランサムウェア」**の被害が一番多く、身代金を払ったとしてもデータが完全には復旧せずに業務に支障をきたすケースや、登録されているメールアドレスから取引先にウイルスに感染したメールが勝手に発信されて取引先にまで被害が及ぶケースが頻発しています。

トヨタ関連の被害のように比較的セキュリティの甘い中小企業に侵入し、より大きな企業を狙う**「踏み台攻撃」**も発生しています。インターネットで**「なりすましメール　お詫び」**と検索すると驚くほど多くの企業がお詫びのお知らせを行っています。社員の PC が感染し多数の取引先にウイルスに感染したメールが、自社の社員の名前で発信された事へのお詫びの文書です。

ネット上にはなりすましメールのお詫びの「文面事例」なるものまで掲載されている始末で、いかに被害が頻発しているのかが伺えます。

被害に遭う事で信用低下も

２月 22 日の日経新聞では、“投資家が企業のセキュリティー対策にも厳しい目を向け始めた”とありました。米国のウーバーテクノロジー社やシンガポール・テレコム社などサイバー攻撃を受けて被害を出した会社の株価が、発生後１年を経過しても被害に遭わなかった企業と比較して大きく下がっているという主旨の内容でした。

株式上場していない中小企業の場合には、投資家を取引先と置き換えて考えれば**「被害に遭った企業の信頼は大きく失墜し取引に長く影響を与えかねない」**とも考えられます。

100%被害を防ぐ事は難しいですが、日頃より可能な限りの対策と定期的なチェック、そして被害が発生したときの対策としての保険は必須と言えるでしょう。

昨年４月の個人情報保護法改正以降、多くの会社でサイバー攻撃対策のお話をさせて頂きましたが、２社に１社以上の割合で取引先から不審なメールを受信し、幸いにもメールを開かなかったために感染を免れた。というお話を頂きました。そのような状況をセキュリティの世界では「インシデント」と呼ぶそうですが、日本語で「ヒヤリ・ハット」という意味に似ており、事故（アクシデント）に対して、「事故未満ではあるが、事故が起こりえる状況に遭遇した」という事です。
日常業務のすぐ水際まで、危険な「インシデント」が発生しています。

被害を最小限に抑え、信用低下のダメージを防ぐために

サイバーセキュリティの世界も予防と対策が必要で、
自動車の運転で言えば“**予防**”とは「安全運転」であり「安全装備」です。
ただ、最新の安全装備が付いた車に乗り、細心の注意で安全運転していたとしても時として事故に遭ってしまいます。予防はするに越したことはありませんが、交通事故と同じで予防しても 100%事故を防ぐ事は不可能で、そのための対策に自動車保険があります。

自動車保険と同様に事故の“**対策**”として、サイバー保険の加入が米国では加入率 50%超と当たり前の世界になってきております。日本においても昨年の法改正により企業の責任が重くなったことにより、データはまだ出ていませんが現場の感覚では非常に多くの企業が加入されています。

サイバー攻撃の被害額はパソコン 1 台につき 100 万～200 万円、総額で 1,000 万円を超える事故も発生しており、利益の喪失とその後の業績悪化が長く続く事を考えると、**自動車保険 1 台程度の費用で加入可能なサイバーリスク保険**は今後、企業にとって必須と言えるでしょう。

技術革新の速い時代、変化に素早く対応する事が求められます

日本の自動車保険は今年で 109 年目を迎えました。大正３年（1914 年）当時、国内を走る自動車は 1,000 台程度だったそうですが、現在では 7,830 万台の自動車が登録されており、自動車保険の普及率も 90%を超えています。ただ、10%は無保険が現状です。

比較して、スマートフォンは 2010 年に 4.4%だった普及率が、2022 年に 94%に達したそうで、わずか 10 数年で一気に普及しました。変化のスピードが一桁違う世の中になり、
サイバーリスク保険の普及も昔の自動車のように 100 年と言うスピードではなく、
スマートフォンと同じで 10 年 20 年のスパンで一気に普及しそうな予感がします。

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