マネジメント講座

サイバーリスク対策入門 ①

誰もが攻撃の標的に

近年、サイバー攻撃が増加しており、２０１７年を振り返ってみても、標的型攻撃、ランサムウエア「ＷａｎｎａＣｒｙ（ワナクライ）」、ビジネスメール詐欺などによって甚大な被害が出たことは記憶に新しいところである。国内では２０２０年にかけて様々な国際的なスポーツイベントが開催予定であり、企業や組織を狙うサイバー攻撃は、さらに増加するといわれている。

一方、サイバー攻撃に関連するニュースが報道されても、特に中小企業では「狙われるのは知名度の高い大企業だけで、自分の会社を狙ったサイバー攻撃はありえない」と捉える企業が多い。しかし、近年では、セキュリティー対策が強固な標的企業に直接サイバー攻撃を仕掛けるのではなく、まずは対策の不十分な関連子会社や取引先の中小企業を狙い、そこを踏み台として標的企業の内部に侵入するケースが増えている。悪意のある攻撃者から踏み台として利用されたとしても、顧客や取引先にとっては自らが直接の加害者となるため、顧客対応や取引先への損害賠償などの被害が甚大になる可能性がある。「自分の会社に限って」という安易な思い込みで対策を後回しにすることは、攻撃者に付け入る隙を与え、自らを積極的に危険にさらすことに他ならない。

今や誰もが巻き込まれる可能性のあるサイバー攻撃は、全ての企業や組織にとって事業存続を脅かす重大な経営リスクであり、重要課題の一つとして認識すべきものとなっている。中小企業であっても「自分の会社は無関係」と思い込まず、サイバーセキュリティーを将来の事業活動の維持・成長に不可欠な「投資」と位置付けて、自らのサイバーリスクを評価し、計画的にセキュリティー対策を講じ定期的な評価・監視を行っていくことが肝要である。

（ＳＯＭＰＯリスケアマネジメント取締役　宮崎義久）

最近のサイバー攻撃の動向

攻撃目的	金銭目的・テロ
攻撃手法	◦高度な標的型攻撃 ◦ＤＤｏＳ攻撃 ◦ランサムウエア
攻撃動向	◦不特定企業への攻撃ではなく特定の組織などを狙った悪質・巧妙な標的型攻撃が急増 ◦公的機関や大企業だけでなく、地方自治体や中小企業が攻撃の標的に ◦ランサムウエアによる標的型攻撃やＤＤｏＳ攻撃のサービス化（アンダーグラウンドサービス）が進行 ◦ＩｏＴ機器（例：ルーター、デジタルビデオレコーダーなど）を踏み台としてＤＤｏＳ攻撃の増加 ◦国際的なスポーツイベントに向けて攻撃の激化が予想

（注）ＳＯＭＰＯリスケアマネジメント作成

2018年5月29日
日経産業新聞