SOMPO未来研究所 主任研究員　内田 真穂氏

デジタル時代のリスクと保険（2）

身代金補償、引き受け中止も

デジタル時代の新たなリスクの代表とも言えるサイバー攻撃。その中で近年急増しているのが、企業を標的にしたランサムウエア（身代金要求型ウイルス）だ。

ランサムウエアは企業のサーバーやパソコンに保存されているデータを暗号化し、それを解除するのと引き換えに金銭（身代金）を要求するプログラムである。感染するとデータが利用できなくなったり、画面がロックされて端末が利用できなくなったりする。暗号化以外にも、データを暴露すると脅す手口がある。

被害を受けた企業の約半数が身代金の支払いに応じている実態も明らかになった。米セキュリティー大手プルーフポイントが主要7カ国の3600の企業・団体に実施した調査によると、2020年に66%がランサムウエアに感染し、うち52%が身代金を支払ったと回答した。国別では米国が87%と最も多く、英国59%、ドイツ54%と続き、日本も33%あった。

攻撃の標的になっているのは大企業だけではない。警察庁の21年上半期の報告では、届け出のあった61件の被害のうち40件（66%）が中小企業だった。

多くの企業が身代金の支払いに応じてしまうのは、システム復旧に日数を要する場合が多く、顧客や取引先に被害が及ぶなどの事情がある。また、復旧には高額な費用を要し、身代金を支払うほうが安くすむケースが多いのも要因である。警察庁の報告では、調査・復旧費用が1000万円以上となったケースが15件（39%）あった。

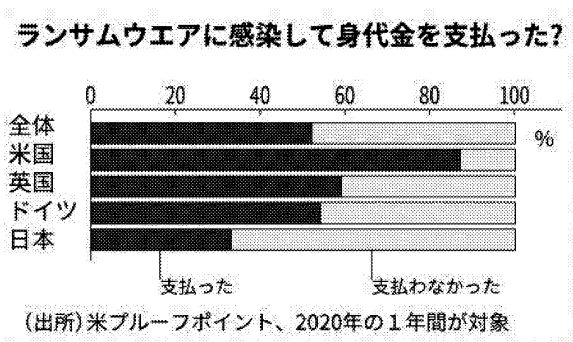
これらに加えて、企業には事業停止による利益喪失やブランド価値毀損などの損害が発生する。米サイバーセキュリティー会社サイバーリーズンが7カ国1263人のセキュリティー専門家を対象に実施した調査によると、3分の2（66%）がランサムウエアによって大幅な収益減を余儀なくされ、半数以上（53%）が企業のブランドが損なわれたと回答した。また、4分の1（25%）が組織の閉鎖を余儀なくされたと回答した。

だが、安易な身代金の支払いは脅迫行為を勢いづかせる。身代金を支払った企業は犯罪者の間で情報が共有され、再び攻撃の標的になりやすい。身代金を支払った企業の80%が再度攻撃を受けているという報告もある。身代金の支払いに一度応じてしまうと、何度も攻撃されうることを経営者は認識しておくべきだろう。

被害の増加を受けて、海外では身代金自体を補償するサイバー保険が販売されている。ただ、保険による身代金の支払いが急増した結果、保険料が上昇する事態も発生している。また、サイバー保険の身代金に対する補償が企業の身代金の支払いを後押しし、攻撃を助長しているという指摘もある。仏大手保険アクサは5月、同国内で身代金を補償する保険の販売を停止することを表明している。

ランサムウエアに限らず、サイバーリスクはデータの蓄積が少ないことに加え、手口なども変わりやすく、リスクを正しく評価して適切な保険料率を算出することが難しい。

さらに保険会社や再保険会社にとってより大きな課題は、集積リスクの問題である。自然災害と異なりサイバー攻撃は世界中で同時多発化する可能性があり、巨大地震災害に匹敵する損害額に上るという試算もある。将来的には官民連携によるリスク負担の検討も視野に入ってくるだろう。



（出所）米プルーフポイント、2020年の1年間が対象

掲載日 2021年11月25日 日経産業新聞 012ページ