加害者にならないためのサイバー攻撃防止法（第5回）

# ますます拡大。身代金ウイルス被害

2017.05.24

インターネットを通じてウイルスを送り込む悪意を持った第三者に、システム内のデータを暗号化され、その復元と引き換えに金銭を要求される被害が急増している。「ランサムウエア」と呼ばれる“身代金要求型”ウイルスが企業の大きな脅威となっている。

## ランサムウエアの被害が収まらない

インターネットを通じてシステム内に侵入したウイルスは、端末内部でデータの改ざん、消去、複製といったさまざまな動作を行う。その中で、ここ数年かつてない勢いで拡大しているウイルス被害がある。「ランサムウエアによるデータ暗号化や端末操作不能」だ。

ランサムウエアとは「ランサム（身代金）」と「ソフトウエア」を組み合わせた造語。攻撃者はターゲットの端末にランサムウエアを感染させ、データを暗号化する。その後ターゲットにメールで連絡し、「データを復元するためには金銭を支払え」と要求する。暗号化されたデータは、攻撃者があらかじめ決めた手順で「復号」しないとアクセスできない。これはまさにデータを人質にした脅迫そのものだ。

ランサムウエアには大きく分けて、端末内に保存されているデータを暗号化するタイプと、端末自体を操作できない状況にするタイプの2種類に分類される。このうち、最近被害が増加しているのは前者。従来型のウイルスで見られたデータの送信、改ざんといった行為は行われない。

ランサムウエアは一般的なウイルスと同様、主にメールに添付されたファイルを開くと感染する。亜種がいくつもあるので感染後の動きはさまざまだが、「ファイル暗号化型ランサムウエア」の一例を示す。まず、感染した端末内に暗号化のための「鍵」を自動作成する。次にその鍵を使って、対象となるファイルを次々に暗号化する。

ファイルを暗号化した後、その鍵は自動的に攻撃者に送られる。これでデータを復元する鍵は攻撃者しか持っていない状態になる。ターゲットに感染を知らせるとともに、身代金要求画面を表示する。被害者は攻撃者からデータ復元用の鍵を入手するため要求に応じる、つまり金銭などを支払うという仕組みだ。

## “身代金”を払うか払わないか… 続きを読む