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

情報セキュリティー大手のトレンドマイクロが2017年1月に発表した「2016年国内サイバー犯罪動向」速報版によると、「2016年1月～11月の期間のランサムウェアの国内被害報告件数は2,690件に上り、前期比（2015年1月～12月：800件）で約3.4倍に増加」している。日本のIT戦略づくりに取り組むIPA（情報処理推進機構）は同年1月、増え続ける被害への対策をまとめたレポート「ランサムウェアの脅威と対策」を発表した。レポートではランサムウエアに関する情報を紹介するとともに、2016年3月、IPAに多くの問い合わせが寄せられたランサムウエア「Locky」感染によって実際に送付された金銭要求画面を掲載。具体的な被害例を挙げながら対策を提示している。

被害の拡大が収まらない要因の1つとして、金銭要求に応じてしまう企業の存在が挙げられる。例えば、2016年には米国の病院が身代金を払って、電子カルテなどのシステムを復旧したと報じられた。トレンドマイクロが実施した「企業におけるランサムウェア実態調査 2016」では、ファイルを暗号化された企業のうち、約6割が金銭要求に応じたという。このショッキングな結果は、攻撃者にとって格好のビジネスチャンスになっていることを示す。

企業が身代金を払おうとするのは、暗号化されたファイルが重要だった場合、要求金額を支払ったほうが被害を小さくできると判断するからだ。暗号化はシステムを破壊するものではない。データ復旧を優先してやむなく要求に応じる企業の行動も理解できる。しかし金銭を支払っても、ファイルが復元される保証はない。容易に金銭を支払えば、さらに犯罪を助長する結果につながる恐れがある。

最低限の対策としてデータをバックアップ

すべての企業にとって、データの安全な管理は重要なテーマだ。ランサムウエアはデータを盗んだり壊したりするのではなく、「人質に取る」のが目的だ。攻撃者の目的は、明確に「金銭」である点が特徴といえる。このような新手の犯罪にどう対処すればよいのだろうか。具体的な方法をいくつか挙げてみよう。

第1は「感染させない」だ。「OSやウイルス対策ソフトを最新の状態に保つ」「不審なメールの添付ファイルは開かない」「メールに記載されたURLを安易にクリックしない」。こうした情報セキュリティーの基本的な対策の徹底がまずは大切だ。

第2に、感染を予測した上で、被害を最小限に防ぐ対策も求められる。ランサムウエアによる暗号化の被害は、クラウド上にもデータを保管するなどネットワーク外にバックアップを確保すればある程度リカバリーが可能になる。現在の管理体制を再確認し、暗号化されてもデータを復元できる体制を検討する必要がある。

ランサムウエアは感染後、しばらく潜伏してからデータを暗号化するケースがある。データ復元のためには、感染前のバックアップデータが欠かせない。最新のバックアップデータだけでなく、その前の世代のデータも保管しておかなければならない。複数世代でのバックアップ管理が不可欠だ。

不正アクセスによる個人情報漏えい事件が大きく報道される中で、ランサムウエアの問題は、ともすると陰に隠れている印象もある。しかし、身代金を払って表沙汰にならなかった事例を含めれば、その被害はすでに膨大なレベルに達しているはずだ。

ランサムウエアの攻撃は相手を選ばない「ばらまき型」が少なくなく、「自社は大丈夫」といった考えは通用しない。パソコンを業務で使うための原則として、すべての企業が危険性を十分に認識し、対策を講じておくべきだろう。