ランサムウェア

ランサムウェア（Ransomware）とは、「Ransom（身代金）」と「Software（ソフトウェア）」を組み合わせた造語で、これに感染したコンピュータをロックしたり、ファイルを暗号化したりすることによって使用不能にしたのち、元に戻すことと引き換えに「身代金」を要求する不正プログラムです。身代金要求型不正プログラムとも呼ばれます。

2017 年 5 月中旬、**WannaCry**（**ワナクライ**。意味は「泣きたくなる」）と呼ばれるランサムウェアによる世界規模の被害が大きな騒ぎになりました。政府機関、企業、個人など、世界 150 ヵ国 20 万台以上のコンピュータの感染が確認され、病院で急患対応や手術が行なえなかったり、工場が操業停止に追い込まれたりといった被害も報道されています。日本では日立製作所や JR 東日本でも被害が確認されています。

ランサムウェアに一旦感染してしまうと、パソコンがうまく操作できなくなったり、パソコン内部あるいはネットワーク共有されているファイルが勝手に暗号化されて利用できなくなったりするので、非常に困った状況になります。仮にランサムウェアを駆除できたとしても、暗号化されたファイルを元に戻すのは困難です。さりとて、攻撃者にお金を払うことは、払ったとしても元に戻る保障はない、そもそも悪の行為を助長することにつながる、お金を払う人間・組織という弱みを握られて形を変えてまた攻撃を受けるおそれが高い、などから、絶対にすべきではありません。

ランサムウェア感染後の画面例（出典：IPA）

ランサムウェアの侵入手口

ランサムウェアの侵入手口は大きくWebとメールの2つですが、2017年に入ってからはWebサイト経由での侵入が目立っています。代表的な手口が、OSやソフトの脆弱性（セキュリティ上の弱点）を攻撃して、端末利用者が気づかないうちにウィルスを送り込む手法です。OSやソフトにセキュリティ更新プログラムが適用されておらず、脆弱性を残したままのパソコンでは、攻撃者が仕掛けを施したWebサイト（正規のWebサイトに攻撃者が侵入し勝手に書き換えている場合もあります）を見ただけでランサムウェアに感染してしまうことがあるのです。

WannaCryはマイクロソフトのWindows OSの脆弱性を突いたものでした。Windowsアップデートを適切に施していれば、修正プログラムによって脆弱性が修正され、WannaCryに感染することは避けられたようです。

最近では脆弱性攻撃に加え、ユーザの油断を誘ってランサムウェアをインストールさせる手口も出現しています。例えば、ブラウザのGoogle Chrome利用者に対して「フォントがインストールされていないため文字化けしている」という趣旨のメッセージを表示し、フォントをインストールするように見せかけて、代わりにランサムウェアを侵入させるという例がありました。

メールを使った攻撃では、メール本文のリンクをクリックさせたり、添付ファイルを開かせたりすることでランサムウェアに感染させる手口が定番です。

ランサムウェアの被害を防ぐための対策

ランサムウェアへの対策は、基本的にウィルスなどのサイバー攻撃に対する対策と同じです。

こまめにバックアップする
一度、ランサムウェアによって暗号化されたファイルを元に戻すことはかなり困難です。重要なデータは、外付けのハードディスクやクラウド上のデータサーバなどにこまめにコピーし、常にバックアップとして保管しておきましょう。

OSやソフトの脆弱性を修正する
パソコンのOSやソフトの脆弱性を残していると、ランサムウェアや他のウィルスなどに感染してしまうおそれがあります。Windowsアップデートを的確に行っておくことは

無論、他のソフトウェアについても開発元から更新プログラムが提供されたら速やかに適用するよう心がけましょう。

メールのリンクや添付ファイルを安易に開かない
ランサムウェアに限らず、サイバー攻撃への対策として、メールの添付ファイルはリンクに気を付けるのは基本です。

セキュリティソフトを最新の状態で利用する
セキュリティソフトを利用すれば、自身で気づくことが難しいメールに添付された不正サイトへのリンクや不正なファイルを検知して感染をブロックしてくれます。新たな脅威に対抗するため、セキュリティソフトは、最新の状態に更新して利用しましょう。