

The following text appeared on the NHK website. For this contest please translate into English all of the portions that appear in blue and omit the portions that appear in red. The translation should be aimed at a general audience; it should be complete, accurate, and as natural as possible. It is not necessary to duplicate the exact formatting of the Japanese text. However, please identify clearly each heading and each paragraph.

世界中で被害「ランサムウェア」

パソコンの中に入っている写真などを読み出せなくし、元に戻して欲しければ金銭を要求するという新しいタイプのコンピューターウイルスが世界中で猛威を振るっています。被害者から金を脅し取ることから「身代金目的」のサイバー攻撃とされています。

どんな被害か

平成28年の3月に蔓延した電子メールに「Document 2」というタイトルのものがあります。差出人は自分で、Document 2.zipという添付ファイルがついています。「自分が送ったメールが届かなくて戻ってきたのかな」と思って、添付ファイルを開いてしまうとウイルスに感染してしまいます。

感染すると、デスクトップに保存していた家計簿や住所録のアイコンが白く変わってしまいました。ファイル名もでたらめになってしまい読み込みが出来ません。調べると、パソコンに保存されていた思い出の写真や、子供の入学式の動画も開けなくなっています。

すると、黒い画像が現れました。「すべてのファイルは暗号化されています。元に戻すには鍵が必要です」。その鍵を入手するには、金銭が必要だということです。大切なデータをいわば人質に、金を脅し取ろうという内容でした。

こうしたウイルスを英語で「身代金」という単語を使って「ランサムウェア (Ransomware)」といいます。要求額は日本円で5～6万円で、ビットコインで支払いを求めてきます。ファイルを自力でもとに戻すことはまず不可能です。ウイルス対策ソフトでウイルスを駆除しても、暗号化されたファイルは元には戻りません。

感染したら金を払うしかないの？

金を払うと元に戻るという報告もありますが、元に戻してもらえなかったという報告もあります。また、つい金を払ってしまう人がいるため、犯罪組織がこのウイルスをばらまき、ビジネスにしているといわれています。こうしたことを考えると、金を払うのは犯罪を助長するうえ、金銭的な被害も被ってしまうことになり、やめた方がいいと専門家は話しています。残念ながらデータは無くなってしまったと思って諦めることになりす。

ランサムウェアは、偽物のセキュリティソフトを販売していたサイバー犯罪グループが利用しているといわれています。偽物のソフトでは金が稼げなくなったため、もっと

暴力的なランサムウェアに移行してきたというのです。金を脅し取ろうとしたとして逮捕された人もいますが、被害が絶えないことを見ると、ランサムウェアを使う他のグループもあると言えます。

情報セキュリティサービスを提供している「キヤノンITソリューションズ」によると、平成28年の3月には、ランサムウェアが添付された電子メールが日本国内に向けて20万通送られたと見られるということです。身代金要求型のウイルスは今後も国内で広がっていくとみられるので、不審な添付ファイルは決して開かないよう十分に注意してほしいと話しています。

「身代金型」のコンピューターウイルスによる被害は、自治体や病院、学校などでも起きています。このうち、東京の町田市役所では去年12月、職員4人に件名や本文がないメールが届き、このうち1人がパソコンでメールに添付されたファイルを開いたところ、ウイルスに感染したということです。ウイルスはパソコンだけでなく、接続されたサーバーや記録媒体のデータまで読み取れなくする仕組みで、ファイルを開いた職員が所属する部署のサーバーのデータが勝手に暗号化され、使えなくなったということです。町田市役所では、データのバックアップを取っていたため復旧できたということですが、一部の業務に影響が出たということです。Twitterには「感染してしまった」という書き込みが多く見られますが、情報が流出するわけではないので、企業などは感染しても発表しないところが多いと見られます。

ランサムウェアの被害を防ぐには

何よりもウイルスに感染しないようにすることです。ランサムウェアは電子メールの添付ファイルで届くことがあります。企業の名前から届いたように見える偽のメールなどで、本物かどうか見分けが付きにくいものが増えています。自分に関係があるメール以外は、決して添付ファイルを開かないようにして下さい。

ウイルスは普通のホームページを閲覧しているうちに感染してしまうこともあります。企業の公式ホームページや、旅行サイト、ネットショッピングなど、いつも閲覧しているホームページで感染してしまうのです。知らないうちに、それらのホームページが改ざんされ、ウイルスをばらまくようになっていることがあります。セキュリティ会社の「トレンドマイクロ」は、平成27年10月に国内の70のホームページが改ざんされ、ランサムウェアをまき散らすようになっていたと発表しています。

もちろん、最新のウイルス対策ソフトを使うことも重要です。

感染を防ぐ対策とともに必要なのは、日頃からデータのバックアップをしておくことです。定期的にUSBメモリーや、CD、クラウドサービスにコピーしておくといいです。もし、データが暗号化されてしまった後でも、戻せば実際の被害を防ぐことができます。そもそもパソコンの内のデータは、操作ミスや何らかのトラブルで消えてしまうこともありますので、定期的にバックアップを取る習慣をつけることは無駄ではありません。