大切なファイルが人質に！

身代金要求型ウィルス！ランサムウェアに感染しないために！

ニュースなどでランサムウェア「Locky」が取り上げられ話題となったことは記憶に新しいと思います。多くのコンピューターウィルスは、使用者から隠れてパソコンに潜み悪さを行いますが、ランサムウェアはパソコンやファイルを人質にして、使用者に金銭を要求してきます。このようなウィルスは6年間で約182倍に増加しているといわれ、手口も巧妙になっています。今回は、このランサムウェアの手口や感染経路、もしもの時の為に今日から行える対策をご紹介していきます。

そもそもランサムウェアとは？　もし感染してしまうと・・

ランサムウェアとは、**感染したパソコンをロック**したり**ファイルを使用不能**にして、**それらの復帰と引替えに身代金（Runsum）を要求するウィルス**です。ある日突然、パソコン画面が脅迫文と共にロックされたり、パソコン内のファイルが全て「〇〇〇.vvv」や「〇〇〇.kkk」となってしまい使用することができなくなります。この状態のファイルは暗号化されていて、たとえ身代金を支払っても暗号化が解除される保証はありませんので、**要求に応じる事の無いように注意してください**。
パソコンを盾に金銭を要求するこの様な手口なので、ランサムウェアは**「身代金要求型ウィルス」**と呼ばれることもあります。
この名称をニュースなどで聞いたことがある方も多いのではないでしょうか？
企業や個人に関わらず感染する恐れがあるので、大事な資料から家族の思い出の写真まで、全てのデータが目の前で使用不能になる可能性がある非常に怖いウィルスです。

感染はどこから？　まずは、敵を知ること

ランサムウェアの感染経路は主に、2通りあります。

【1】ウェブページ閲覧による感染

危険なサイトにアクセスしなければ大丈夫、と思われるかも知れませんが、昨日まで問題がなかった普通のページでも、不正に改ざんされてある日突然ウィルスをばらまくこともあります。また、ページ広告などから感染する場合もあります。一般的に広告はランダムで表示されることも多いため、運悪く感染してしまうこともあるかもしれません。

【2】スパムメールによる感染

怪しいメールは全て英語で関係ない、と切り捨てられましたが近年は日本語によるスパムメールも多くなっており、今後も増加すると考えられます。大手企業を名乗り、文面も特別おかしくない･･･でも実際はスパムメールだった！ということも十分にありえます。

これらはセキュリティソフトが防いでくれる場合もありますが、自分自身での予防・対策も重要です。

予防と対策をチェック！

スマートフォンでも要注意

コンピューターウィルスの話は、スマホには関係がないと思われがちですが、今年の3月にAndroidスマホの日本語版ランサムウェアが確認されています。こちらは、不正なアプリをダウンロードすると、スマホがロックされて使用不可能になってしまうというものです。今後は、スマートフォンでも右の表を意識するほか、アプリのダウンロードにも気をつける必要があります。

感染の予防と対策

感染経路	感染経路
【1】ウェブページ閲覧による感染 	使用しているOSやブラウザ、FlashPlayerなどが古いとそれだけで感染してしまうリスクが高まります。OS・ブラウザ・FlashPlayerの更新は、こまめに行い、常に最新の状態にしましょう。もちろんその他にも使用しているアプリの更新があった場合、そしてそれがセキュリティに関係するものだった場合は、速やかに更新を行うことを強くお勧めします。自動更新の設定が行える場合は、有効にしておくといいでしょう。
【2】スパムメールによる感染 	心当たりのないメールの添付ファイルは絶対開かず削除すること、URLは絶対クリックしないこと、この2つが最も重要です。近年は巧妙なスパムメールも増えているので、注意が必要です。日本郵政や大手運送会社、通販サイトなどを名乗り、請求書や追跡番号と偽り、添付ファイルを開封させようと誘導します。メールアドレスも本物に近い形で詐称していることが多く、一見するとわかりにくくなっています。少しでもおかしいと感じたら、むやみに開かず削除しましょう。

セキュリティソフト・ウイルス対策ソフトの更新もこまめに

上記の2点を日ごろから意識した上で、導入されているウィルス対策ソフトの更新もしっかりと行いましょう！

バックアップの重要性！

ランサムウェアによっては感染したパソコンからアクセス可能な全てのファイルを暗号化するものもあり、ひどいものだとデータの破壊・削除まで行います。そうなってしまうと、そのデータを復元することは困難です。ランサムウェアを駆除しても、暗号化・破壊・削除されたファイルは元に戻らないからです。

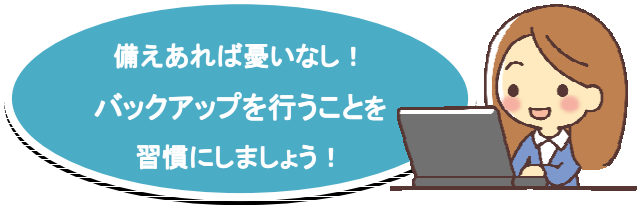
どれだけ対策をしていても、次々と新しいウィルスがでてくるので、最悪の場合の備えも必要不可欠となっています。
最も重要な備えは、データのバックアップです。普段から、障害対策の為にバックアップをとられている方も多いと思いますが、今回ご紹介したランサムウェア等の影響でバックアップの重要性が以前より上がっています。バックアップをとっていれば、バックアップをとった時点へ復元することが可能です。

バックアップ時の注意点

ランサムウェアによる感染に備えて、バックアップ時には以下の点に注意してください。

【1】 バックアップは定期的に、複数で行う。
1日一度行うなど、ルールを決めてこまめにバックアップすることをお勧めします。さらに、クラウドサービスとその他の媒体、複数に行うと良いでしょう。

【2】 バックアップに使用する装置・媒体は、バックアップ時のみパソコンと接続すること。
DVD-R・USBメモリ・メモリーカード・外付けHDDなどを使用する際はバックアップ時のみパソコンに接続しましょう。



開発室から

チョット目を離した隙にWindows10へのアップグレードが勝手に始まってしまった･･･とネットでも大騒ぎになり、マイクロソフトもアップグレードが開始された後のキャンセル手順の動画を公開しました。一度見ておけば、万一の時、慌てる事もありませんよ。ちなみに無償アップグレードは7月28日までですよ。