【ランサムウェア流行】大切なデータが開けなくなります！

世界規模のランサムウェア攻撃が起っており、日本企業も被害に合っています。連日のニュースで気になっている方も多くいらっしゃるかと思います。データの復旧は保証されませんので、事前に感染を防ぐことが最も重要です。
ランサムウェアは主にWindows 環境での感染が確認されていますが、AndroidやMac環境でも確認されているのでどの端末に対しても対策が必要です。

ユーザー様も被害に！

実は昨年、弊社ソフトのユーザー様が被害に遭われてしまいました。（ファイルが開けなくなります！危険なランサムウェアにご注意ください。
USBなどでパソコン内のデータのバックアップはもちろんですが、弊社の平兵衛くんや坪拾いをお使いのユーザー様は、物件データのバックアップに『どこでもデータBOX』のご利用がおすすめです。
パソコンに問題が起きても、安全なクラウド上にデータが保存されます。『どこでもデータBOX』は、利用を有効にしていただくと、作成した物件が自動的にクラウドに保存されます≪設定方法はこちら≫。もしもの時のために、今すぐ設定していただくことをお勧めします。

ランサムウェアに感染するとどうなるか

最近流行しているランサムウェアの感染時の画面です。

· 画面がロックされて操作が行えなくなります。
・パソコンに保存していた写真や動画、ファイルが暗号化され開けなくなります。
・データの復旧のための費用を請求されます。データが復旧される保証はありません。

感染経路

ランサムウェアはメールからの感染がほとんどです。添付のファイルを開いたり URLをクリックすることで感染します。

被害を防ぐために

ランサムウェアの被害を防ぐために、次の対策を心がけましょう。

◆不自然なものには“触らない”

ランサムウェアの被害のほとんどはメールから発生しています。エクセルファイルや圧縮されたデータなどがメールに添付されている、特に見知らぬメールアドレスのもの、英語のメールなどはご注意下さい。中には業務に関連したタイトル名で来ることもありますので、添付ファイルを開く前にメール本文を必ず確認するようにして下さい。

◆OSやソフトの“更新プログラムを速やかに適用”

ランサムウェアの侵入口となるOSやソフトの脆弱性への対策は欠かせませ

ん、Windows Updateやその他ソフトの更新プログラムが提供されたら速やかに適用してください。

◆セキュリティソフトは常に“最新に”

セキュリティソフトを導入していると被害の発生自体を防ぐことが期待出来ます。しかし最新のものでないと効果は薄くなります。実際に、セキュリティソフトを入れられていてもバージョンが古かったことで被害が発生しています。

◆大切なデータは、複数の場所でこまめに“バックアップ”

感染すると元のデータを開くことが出来なくなるため、普段から別の場所にデータのコピーを残しておくことが有効です。この作業をバックアップと呼びます。コピーする先は外付けのハードディスクやCD、DVDといった光メディアなどがあります。ただしパソコンに繋ぎっぱなしにしていると感染した場合に被害を受けるため、普段はパソコンから外しておきましょう。

坪拾いや平兵衛くんで作成されたデータに関しては、『どこでもデータBOX』のご利用がお勧めです。