サイバー防犯通信 No.27

平成29年5月1日
兵庫県警察本部
サイバー犯罪対策課

ランサムウェアの感染に注意!!

ランサムウェアとは

「Ransom(身代金)」と「Software(ｿﾌﾄｳｪｱ)」を組み合わせて作られた名称で、コンピュータウイルスの一種です。
このウイルスに感染すると、パソコン等の端末に保存しているデータが暗号化されて使えなくなったり、スマートフォンの操作が不能となり、その制限を解除するための身代金を要求する画面が表示されます。

感染経路

【主な感染経路】

メールの添付ファイルの開封等

ランサムウェアに感染するよう細工されたメールの添付ファイルの開封や本文中に記載されたURLのクリック

ウェブサイトの閲覧等

改ざんされたウェブサイトの閲覧や、ファイルのダウンロード

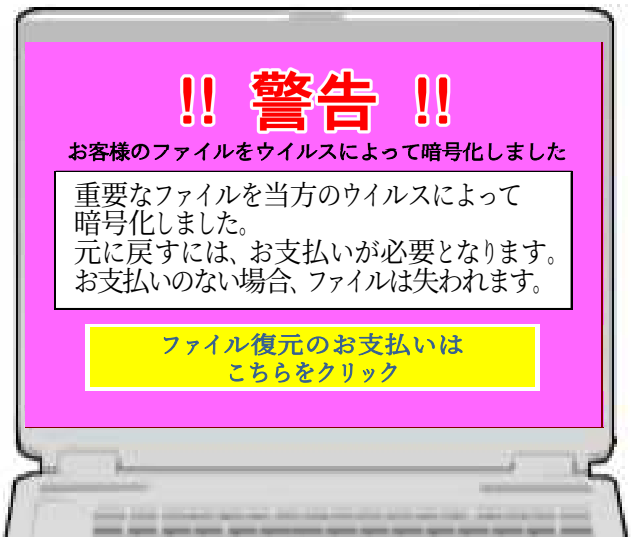
※ サイトにアクセスしただけでウイルスに感染することも!!

ランサムウェアに感染すると…

【暗号化型の場合】
・端末内の文書ファイルや写真などのデータが暗号化され開けなくなってしまいます。
・感染した端末だけでなくネットワーク上で接続された共有フォルダ等が暗号化される場合もあります。

【端末ロック型の場合】
・端末の画面がロックされ使用できなくなってしまいます。
・スマートフォンをロックするランサムウェアも確認されています。

【端末に表示される身代金要求画面イメージ】



※ランサムウェアの種類によって身代金要求画面は異なります。
法執行機関を装った要求画面も確認されています。

対策&感染時の措置は次ページを確認

ランサムウェアの対策&感染時の措置

対　策

● **ウイルス対策ソフトを導入する**
　ウイルス対策ソフトを導入し、定義ファイルは最新の状態に保ちましょう。

● **OS及びソフトを最新の状態にする**
　ＯＳ及びインストールされているソフトウェアを更新し、常に最新の状態を保ちましょう。

● **メール等に注意する**
　知人等からのメールでも、不用意に添付ファイルを開いたり、リンクをクリックしないよう注意しましょう。
　また、動画サイト等を閲覧する際は、不審な広告バナーやダイアログボックス等をクリックしないようにしましょう。

ウイルス付メールの例
「金銭の支払い請求書」
「荷物の配達通知」
「ショッピングの注文確認」
「写真や書類の確認要請」等
※ 添付ファイルの拡張子(.jsや.exe等)にも注意!!

● **重要なファイルは定期的にバックアップ**
　重要なデータは定期的にバックアップを作成しましょう。
　また、外付けのドライブ、クラウド上に保存するなど、バックアップは複数作成した上、外付けのドライブは必要なとき以外は外しておき、クラウドはファイルを同期しないようにしておきましょう。

もし、感染したら…

○ **ランサムウェアの名前等を検索し、情報収集**
　暗号化されたファイルの拡張子や画面に表示されている脅迫の文章等をインターネットで検索しましょう。
　ランサムウェアの種類によっては、ウイルス対策ソフト事業者等から復号ツールが提供されていることがあります。

○ **「システムの復元」機能の検討**
　WindowsOSの「システムの復元」機能を利用して感染以前の状態に復旧できる可能性があります。ただし、「復元ポイント」以降に作成されたデータは復元されません。またランサムウェアの種類によっては復元ポイント自体を暗号化したり、破壊して無効化するものもあります。

○ **復号ツールの利用**
　ランサムウェアによりファイルが暗号化された場合、一部のランサムウェアについては復号ツールが公開されており、暗号化されたファイルを復号する手段として復号ツールの利用が考えられますが、以下の点に注意してください。

慌ててお金を払ってしまう前にまず確認！！

・　復号ツールが対応しているのは、一部のランサムウェアです。
・　復号ツールが利用できるランサムウェアとして紹介されていてもバージョンが異なれば復号ツールが利用できるわけではありません。
・　復号ツールは提供元の企業からの保証等がなく、予期せぬ不具合が生じる可能性があります。

参考：一般財団法人日本サイバー犯罪対策センター(ＪＣ３)のウェブサイトにおいて復号ツールの利用方法を紹介しています。

セキュリティ意識を高めて被害防止に努めましょう