

ランサムウェアにご注意を!!

～身代金要求型不正プログラムについて



ランサムウェアとは

ランサムウェアは、身代金要求型不正プログラムと呼ばれるコンピュータウイルスです。最初に、パソコンのファイルを暗号化したり、スマートフォンをロックして使用不能にしてしまいます。次に、大切なファイルやスマートフォンを人質にとり、元の状態に戻すことを引き替えに金銭（身代金）を要求してくるもので、その感染が拡大しています。

どうやって感染するか

ランサムウェアは一見自分の業務に関係ありそうな、思わせぶりなタイトルを付けて送信されます。例えば、「業務連絡」「おたずねの件について回答します」「先日お見積もりいただいた件」といったものです。このメールには「××の調査結果」「アンケートの概要」「見積書」などのタイトルのファイルが添付されていますが、実はこれがランサムウェアの実体です。これらのメールの添付ファイルを直接実行したり、パソコン内に保管して開こうとすると、ただちに感染します。また、スマートフォンでは、無料で利便性をうたうアプリなどを怪しげなサイトからダウンロードし、それをインストールすると感染するタイプも増えています。

感染するとどうなるか

ランサムウェアに感染すると、パソコンの場合は、ドキュメント・フォルダやデスクトップなどに保存された文書や写真などのファイルが次々と暗号化され、ファイルを開くことが出来なくなります。中には、パソコンをシステムごとロックしてしまうタイプも存在するようです。スマートフォンが感染すると、画面をタップしても全く操作ができなくなり、たとえ電源を落として再起動しても使えないままの状態は変わりません。どちらの場合もファイルや端末が使用不能の状態のまま、画面には、金銭を要求する表示と支払期限までのカウントダウンが刻まれます。



ファイルが暗号化されてしまったパソコンの例

身代金の要求

パソコンのファイル暗号化やスマートフォンのロックが完了すると、画面上に「警告！」「あなたのファイル（端末）は暗号化（ロック）されました」などのタイトルで「元の状態に戻したいのなら、〇万円支払う必要がある」旨が記載された画面が表示されます。金銭の要求方法は、ギフトカードであったり、仮想通貨であったりとさまざまです。しかし、この画面の指示に従ってお金を支払っても元に戻る保証はどこにもありません。



身代金要求画面の例(スマートフォン)

予防と対策

- ・ウイルス対策ソフトをインストールする。
- ・OS やアプリケーションを常にアップデートしておく。
- ・感染しても自力で復旧できるようにバックアップを欠かさない。
- ・怪しいメールに添付したファイルは開かない。
- ・怪しいメールの本文中にあるリンクをクリックしない。
- ・スマートフォンのアプリは Google Play 等公式サイト以外からはダウンロードしない。