怪しいメール ランサムウェアに 注意!

ランサムウェアとは、感染したコンピュータをロックしたり、ファイルを暗号化したりすることによって使用不能にしたのち、元に戻すことと引き換えに「身代金」を要求するマルウェアです。

主にメールの添付ファイル、リンクURLなどを経由して感染します。

感染しないための 対処、対策

※※知り合いからであっても違和感のあるメールの※※

添付ファイルを安易に開かない

※※マイクロソフトオフィスや他アプリの※※

「コンテンツの有効化」や「編集を有効にする」を安易に押さない

※※特殊な拡張子を開くための※※

アプリをインストールしない

「怪しいメール」の特徴

以下など、巧妙な方法で感染させようとするので当てはまる場合は注意してください。

1. 公共機関や大手サービスからのWebサイトに誘導する為の案内
2. 大手サイト等からの突然のパスワードのリセットの報告
3. フリーのメールアドレスからの送信
4. 英文が多い
5. 日本語の文章として破綻している
6. 極端に本文内容が少ない

過去にやりとりのある相手からのメールでもウィルスメールが送られてくる事もあるので注意!!

「おかしいな?」と思ったら、まずは周囲に確認しましょう!

※万が一「ランサムウェア」を開いてしまった場合は ...

- 身代金要求のメッセージウインドウが出た。
- 画像をクリックしたのになぜが画像が出ない。
- 変なダイヤログ、真っ黒なウィンドウが出た。
- おかしなサイトが開いてしまった。
- ファイルにアクセス出来ない、または警告が出る。

... などの場合「ランサムウェア」を開いてしまったと思ってください。

上記の症状がある場合、以下対処をしてください。

ネットワークから切り離す

感染に気づいたときは、パソコンに繋がっているドライブも被害に遭う可能性があるため、すぐにネットワークから切り離してください。
素早く対処すれば、すべてのファイルが暗号化される前に拡散を防げます。

PCのLANケーブルを抜く、Wi-Fiを切断する
※必ずこれを最初にやってください!

PCの再起動はしない

一度シャットダウンした

ランサムウェアに感染している場合、再起動すると症状が悪化する危険性があります。
将来的に復元ができる可能性があるため、再起動ではなく休止状態にするハイバネーションを実施し、専門家に見てもらいましょう。

セキュリティソフトを利用

セキュリティソフトを利用している方は、一度検知させてみるのがおすすめです。
その時点でランサムウェアを駆除できる可能性もあるためです。
一方で、セキュリティソフトを利用していない人はこれを機にセキュリティソフトの導入を検討してみてください。
サイバー攻撃を受けないための怪しいサイトへのアクセス防止や、ウイルスの駆除もセキュリティソフトで対応できます。
最悪の事態を防ぐためにもセキュリティソフトを入れておくことが重要です。