



サイバー犯罪対策通信

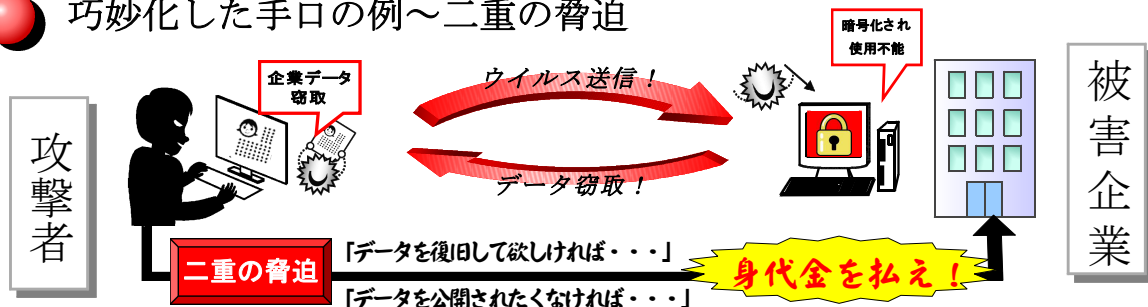
和 泉 警 察 署

ランサムウェアにご注意！

パソコン等のデータを暗号化し、復旧と引き換えに身代金を要求する「ランサムウェア」と呼ばれるウイルスの手口がさらに巧妙化し、被害が増加しています！

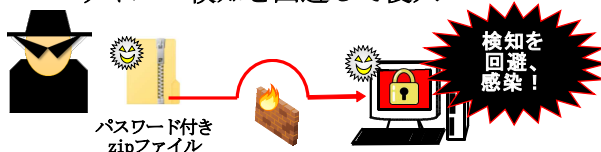


巧妙化した手口の例～二重の脅迫

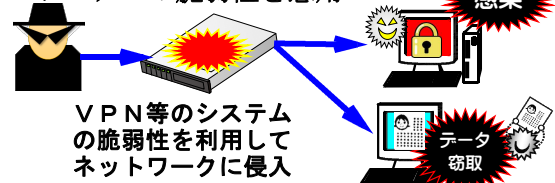


感染手口も巧妙化！

“パスワード付きZIPファイル”で
ウイルス検知を回避して侵入

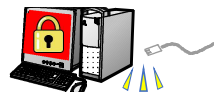


リモートワーク等で使用される
システムの脆弱性を悪用



ランサムウェアに感染してしまったら

- ◆ 感染端末をネットワークから
隔離する
(電源は落とさない)



LANケーブルを抜く



無線LAN機能を無効にする

※ 会社のセキュリティ担当者又は情報セキュリティ関係の会社への連絡も併せて行ってください

- ◆ セキュリティベンダー各社が
提供している復元ツールでの
復元を試みる

(参考)

トレンドマイクロ「ランサムウェア ファイル復号化ツール」
<https://esupport.trendmicro.com/support/vb/solution/ja-jp/1114210.aspx>

- ◆ パソコンの
「システム復元」
機能を使う



→ いずれの方法も完全な復元を保証するものではありません。



サイバー犯罪に関する情報提供を受け付けています！

「大阪府警察ホームページ」<https://www.police.pref.osaka.lg.jp/>