



PCの異変・ウイルス感染が 疑われるとき

(社内保管用 / 配布版)



※ 怪しい画面が出た・ランサムウェア(身代金要求)が出た・不審な添付ファイルを開いた時は、自己判断せず以下の手順を即座に実行してください。

STEP 1 【10秒で実行】

社内ネットワークを今すぐ切る！

他のパソコンや会社のサーバーへの感染拡大を食い止める最優先の作業です。

有線LANの場合



パソコンの横や裏にある「LANケーブル」を指でつまみを押して引き抜く

Wi-Fi(無線)の場合



画面右下の「Wi-Fiマーク」をクリックして「切断(オフ)」にする

※ ノートPC本体に「Wi-Fiスイッチ」がある場合は、スイッチをOFFにする

STEP 2 【注意】

パソコンの電源は「絶対に落とさない」！

過去の対処法(電源を切る)は現在NGです。電源を切ると犯人の手がかりが消えてしまいます。

- ✗ 電源ボタンを長押しして強制終了しないでください
- ✗ コンセントを抜かないでください

理由

メモリに残っている暗号化解除の手がかりや、侵入経路の証拠データが消去されてしまうためです。

※ 異臭・発煙など物理的な危険がある場合のみ、電源プラグを抜いてください。



STEP 3 【記録】

表示されている画面をスマホで撮影する

専門エンジニアが調査・復旧するために重要な情報源になります。



- ・ スマホのカメラで、パソコン画面全体をそのまま撮影してください。
- ・ 画面に出ている英文・警告文・カウントダウンタイマー
- ・ 直前に開いたメールの送信者・添付ファイル名・クリックしたリンクURL
- ・ 発生日時(何時何分頃に起きたか)

STEP 4 【報告】

以下の緊急連絡先へすぐに電話する

「怒られるかもしれない」と隠すのが一番危険です。初動が1時間遅れると全社のデータが消滅します。早期報告は一切不問です。

優先順位	連絡先・担当役職	担当者名	電話番号 / 内線
第1報	社内セキュリティ責任者(情シス / 総務)	[]	内線: [] 携帯: [- -]
第2報	直属の上長	[]	内線: [] 携帯: [- -]
第3報	外部保守・ITサポート窓口	[]	TEL: [- -] (契約番号:)

※ 第1報の担当者が不在の場合は、迷わず第2報・第3報へ連絡してください。



【厳禁】現場の自己判断でやってはいけない3大NG

1



身代金要求画面のリンクをクリックしたり、攻撃者に連絡メールを送る
(詐欺・二重要求の標的になります)

2



バックアップ用の外付けHDDやUSBメモリを接続する
(差し込んだ瞬間にバックアップまで暗号化されます)

3



ウイルスソフトの「スキャン」や「削除」を勝手に実行する
(ウイルスの痕跡が上書きされ、被害状況の調査ができなくなります)