パソコンがおかしい、ファイルが開かない、脅迫の画面が出た

サイバー攻撃かもしれません。最初の 3 手を、その場でしてください。

1

切る

その端末の LAN ケーブルを抜く。無線なら Wi-Fi を切る。広がる通り道を断つ。

2

止めない

電源を切らない。再起動しない。痕跡が消えると原因が分からなくなる。

3

記録する

画面を写真に撮る。気づいた時刻、部署、機器、誰が何をしたかを紙に書く。

責任者に伝えること 5 つ

- 発生部署（どこの部署か）
- 発生箇所（どの機器か。管理番号か画面の名前）
- 日時（いつ気づいたか）
- 連絡者（自分の氏名と内線、携帯）
- 異常の状態（画面の文字、動かない操作、見慣れないファイル名）

してはいけないこと

- 電源を切る、再起動する
- 脅迫の画面の指示に従う、連絡する、支払う
- USB メモリで別の端末にデータを移す
- 自分で直そうとして操作を続ける

連絡先（院内で記入）

部門責任者	＿＿＿＿＿＿＿＿ 内線 ＿＿＿＿
医療情報システム安全管理責任者	＿＿＿＿＿＿＿＿ 携帯 ＿＿＿＿＿＿
夜間休日（当直師長、事務当直）	＿＿＿＿＿＿＿＿ 内線 ＿＿＿＿
電子カルテのベンダー（保守窓口）	＿＿＿＿＿＿＿＿ 夜間休日 ＿＿＿＿＿＿
厚生労働省 医政局医療情報担当参事官室	03-6812-7837（外部への連絡は責任者が行う）

出典: 厚生労働省「【医療機関用】サイバー攻撃を想定した BCP 策定の確認表のための手引き」（令和6年6月）の初動対応と検知の項目をもとに作成。作成: 病院ドック（株式会社ウェブリク）https://byoin-dock.jp/tools/cyber-security/ 2026-09-25