ランサムウエアに感染！どうする？

脆弱性のあるＶＰＮ機器等から感染！！

感染例

機器のアップデートが行われておらず、脆弱性が残ったままＶＰＮ機器が原因で犯人が社内のネットワークに侵入

社内ネットワークを通じて感染が拡大し、業務用パソコンや同じネットワーク内に保存されているバックアップデータも感染被害に！

ＶＰＮ等のセキュリティ機器は常に最新の状態を保ちましょう！

バックアップデータはネットワークから切り離して保管を！

データを暗号化されたら？

　感染端末をネットワークから隔離

　　復号に必要なデータが残っている場合もあるので電源は切らない！

　至急セキュリティ担当者に報告

　　有事に備えて予め担当者を決め、連絡体制を確立しておく！

　速やかに警察に通報・相談

　　被害拡大を防ぐためにも、被害を隠して潜在化させない！

暗号化されたデータが復元できることも！？

　一部のランサムウエアについては、復合ツールが「Ｎｏ　Ｍｏｒｅ　Ｒａｎｓｏｍ（※）」のウエブサイトに公開されており、暗号化されたデータを複合出来る場合があります。

　　<https://www.nomoreransom.org/>ja[/](https://www.npa.go.jp/bureau/cyber/soudan.html)index.html

※　「Ｎｏ　Ｍｏｒｅ　Ｒａｎｓｏｍ」は、ランサムウエアの被害低減を目指す国際的なプロジェクトです。

その他サイバー犯罪対策に関する事は、大阪府警ホームページをご確認ください。

企業・組織等に向けたサイバーセキュリティ講演も実施中！