ランサムウエア攻撃 に備える

バックアップはシステム上の基本（出来ていないならやりましょう）

理想的なバックアップ方法　（情報処理試験の基本中の基本）

☆ データを３つ保管　（原本 + 最低コピーを2つ）
☆ 異なる２種類の媒体に保存　（例：HDD + クラウド、NAS + SSD）
☆ １つは社内LANから切り離して保管（遠隔地でのバックアップ）

重要なのは定期的な **復旧テストを実施** することが不可欠（月に1回程度）
バックアップが**正常に動作しない場合、復旧が遅れ、業務継続に支障**をきたす恐れがあります。

対策予算が限られている場合

1. 侵入リスクの低減　：ソフトやOSのバージョンアップとパッチ適用の徹底　等　（迅速に）
2. バックアップの徹底　：上記の基本行動
3. 少なくともNGAVの導入　：疑わしい挙動プログラムを自動解析し、事前にブロック。価格に注意
4. インシデント対応の重要性　：攻撃を完全に防ぐことは困難、有事の際の対応計画を策定し
   シミュレーションを行うことが不可欠

攻撃されるリスクに対しては（BCPとして考えてください）

1. 低減：リスクの発生可能性や影響度を下げるための対策（セキュリティソフト導入、社員教育）
2. 移転：リスクによる損失の全部または一部を、第三者に転嫁（保険・アウトソーシング・クラウド）
3. 受容(保有)：リスクを認識した上で、特段の対策を講じずに受け入れ
4. 回避：リスクの原因となる活動そのものを中止・変更

発行：2025年10月20日