

ランサムウェアに**感染**しても 業務を再開できますか？



ランサムウェアは悪意のあるソフトウェアで、データを暗号化し、解除のために身代金を要求するサイバー攻撃手法です。感染したコンピュータだけでなく、接続している外付けHDDやUSBメモリなどのファイルも暗号化され、さらにネットワークを介して会社の基幹システムや他のコンピュータにも被害が及ぶ可能性があります。

外付けのHDDに自動でバックアップを取っているから安心だと思いませんか？

従来のバックアップはランサムウェアに対抗するのが難しい理由がいくつかあります。同期型のバックアップは感染が即座に反映され、オンラインバックアップは感染の影響を受ける可能性があります。また、自動バックアップは感染前のバージョンを上書きすることがあり、バックアップ検知が遅れると有効な復元が難しくなります。

効果的な対策としては、オフラインで保管された定期的なバックアップが重要です。

オフラインバックアップ



RDX



簡 単

USBケーブルでコンピュータに接続するだけで利用できます。ドラッグ＆ドロップでデータのコピーと移動もシンプルに実行できます。なお、外付けドライブはUSB給電で動作します。

選 べ る

RDXデータカートリッジは、500GB、1TB、2TB、4TB、5TBのHDDをご用意しています。データ量の増大など必要に応じてRDXデータカートリッジを増設することで、将来にわたって使用することができます。