I-O DATA

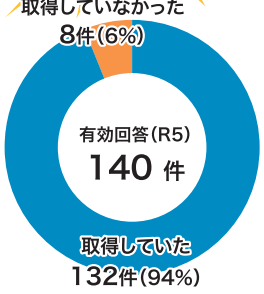
NASご導入のお客様へ

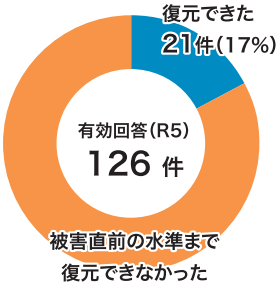
猛威を振るう
身代金要求型不正プログラム
ランサムウェア

被害 **再拡大!** 問い合わせ **急上昇!**

衝撃

ランサムウェア被害にあった企業のうち、80%以上がデータ復旧できていない!!





警察庁広報資料「令和5年におけるサイバー空間をめぐる驚異の情勢等について」によると…

バックアップはほとんどの企業が行っている。
しかし、データを完全に復元できなかったケースが**83%**も発生している。

ランサムウェア対策のためには、
バックアップ設定を適切に行うことが重要です!

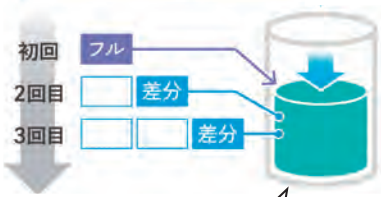
NASを使ったランサムウェア対策バックアップ方法

ランサムウェアに感染したパソコン

1 NAS

2 NASバックアップ用外付けHDD

フルバックアップとは違い、
当社独自の差分バックアップ方式を
使っているので容量は最小ですみます。



差分データのみが保存されるので
容量が節約でき、時間も短縮!

NASに接続したバックアップ先の外付けHDDネットワーク共有を「無効」にしてください。

「エアギャップ(経路遮断)」を実現するオフラインバックアップ設定です。これにより、ネットワーク上のパソコンから、直接バックアップ先の外付けHDD内のバックアップデータにアクセスされることを防ぐことが可能です。

世代管理のできるバックアップ方法で外付けHDDにデータをバックアップしてください。

アイオーのLAN DISKのバックアップ先は、自動的に「読み取り専用」に設定されるため、バックアップデータは、保存期間中は変更不可「イミュータブル(不変)」となります。

さらにランサムウェア対策のバックアップには、
世代数の設定も重要です。

バックアップ世代数や容量の解説と製品ご紹介は【裏面】へ

3世代では不十分!

14世代以上バックアップでランサムウェア対策!

「世代バックアップ」は、ランサムウェア対策として有効な手法の一つ。しかし、昨今ランサムウェアが進化し、潜伏期間が長期化しています。
これまで十分だと言われていた“3世代バックアップ”では、長期化するランサムウェアに対応することが難しくなっています。

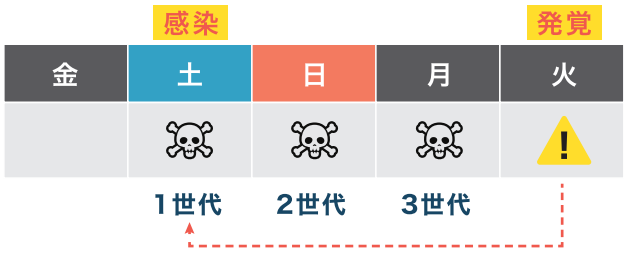
“3世代バックアップ”の落とし穴!

週末に感染しても月曜日に発覚すれば前週金曜日のデータを復元できます。
しかし、発覚が1日でも遅れた場合や、GWや年末年始などの長期休暇中に感染した場合、**復元は不可能**です。
ランサムウェアの潜伏期間が長期化していることもあり、3世代のバックアップだと決して十分とは言えません。

■発覚が月曜日の場合

◎復元可能!

■発覚が火曜日の場合



×復元不可能!(感染前のデータが無い)

いまからでも間に合う! “14世代以上のバックアップ”に変更しよう!

GWや年末年始などの長期休暇や長期化しているランサムウェアの潜伏期間にも対応するため、I-ODATAは二週間分を目安に**“14世代以上のバックアップ”**を推奨しています。バックアップハードディスクの必要容量は、NAS型番の容量数値と同じ容量、実効容量の二倍がおすすめ。既にその分の容量をもつハードディスクをお使いの場合は、簡単な設定手順でバックアップする世代数を変更できます。容量が足りない場合や今からバックアップハードディスクをお求めの場合は、大容量モデルへの買い替えをご検討ください。

■NASとバックアップ先HDDの組み合わせ例と表

NAS
HDL2-HA4B
総容量4TB　実効容量2TB

ハードディスク
HDJA-UTN4B
4TB

NAS総容量	NAS実効容量(出荷時)	バックアップ先容量
2TB	1TB	2TB
4TB	2TB	4TB
8TB	4TB	8TB
12TB	6TB	12TB
16TB	8TB	16TB

買い替えるならこれ! 高信頼性USB接続ハードディスク“BizDAS”

バックアップに便利

HDJA-UTNB シリーズ

USB 3.2 Gen1対応 USB ハードディスク

1TB　2TB　3TB　4TB
6TB　8TB　12TB　16TB　20TB

おすすめ

NarSuS

累計12万台の利用実績をもつ
遠隔管理サービス「ナーサス」

離れた場所から機器の状態を管理できます。
異常時はもちろん、定期的に機器の状態をお知らせします。

株式会社アイ・オー・データ機器　www.iodata.jp

お問い合わせはこちら

平井商会
TEL 0532-63-6461
FAX 0532-61-5782