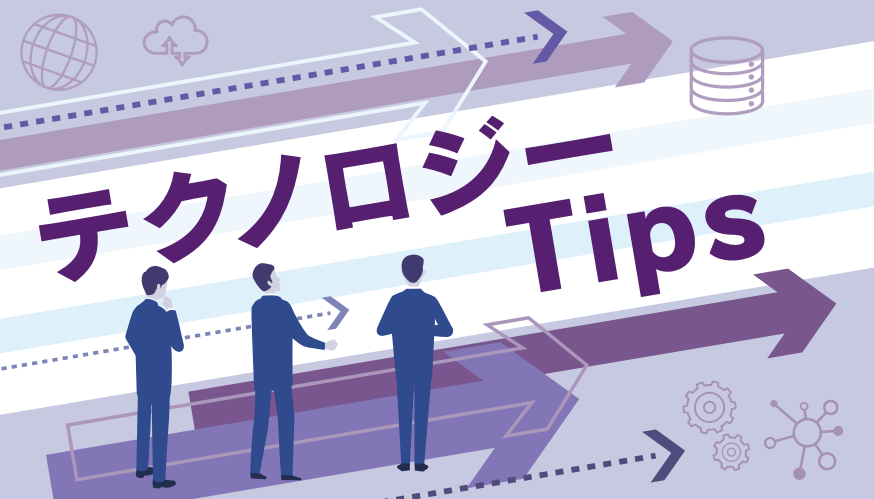




「多発!!」セキュリティインシデント!バックアップは基本であり、重要です。

企業データを守る 「バックアップ完全ガイド」

間違っているかもしれない!?バックアップの認識・方法・管理について整理します。



うちはRAID*を
入れているから大丈夫!



外付けHDDにコピー
しているから安心!



頻繁にUSBにコピー
しているからOK!

もしそう思われているなら、この資料は重要な警告になるかもしれません。

* RAID: 複数ディスクを1つの仕組みとして使い、データの置き方を工夫し速度や故障耐性を高める方式。データを複数台に分けて書く(高速化)、同じデータを複数台に保存する(冗長化)、復元用の情報(パリティ)を含めて保存、故障時に再構成できるようにします。

①バックアップとは?

『いつ』の時点に戻せるか「別の場所」に保管すること

① 隔離

システムが壊れても
影響を受けない場所に保存する。



② 履歴

「昨日」「1週間前」「1ヶ月前」の
状態に戻せるようにする。



この2点が揃って初めて
「バックアップ」と呼びます。
単なるコピーではありません。



②【超重要!】バックアップの意味ややり方、勘違いしていませんか?

多くの企業が陥っている「バックアップだと思っているが、実は無意味(または危険)」な事例です。



×勘違い1 RAID(レイド)があるからバックアップは不要

これが最も多い、致命的な勘違いです。

- RAIDの役割:HDDが故障しても「システムを止めない」ための技術です。
- なぜバックアップではないのか?

誤操作

ファイルを削除すると、RAIDの
全ディスクから瞬時に削除されます。

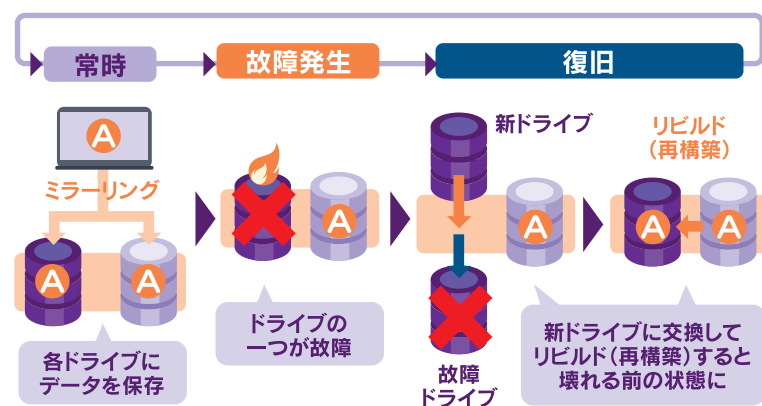
ウイルス

ウイルスに感染すると、
RAIDの全ディスクも感染します。

災害

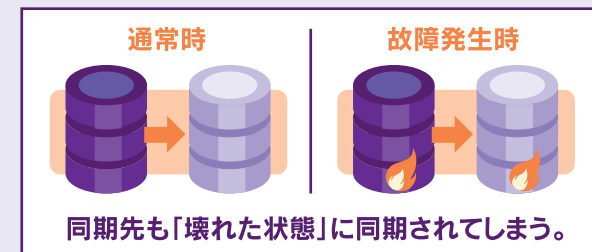
サーバーごと水没・焼失すれば、
RAIDも全滅です。

RAIDはHDDの破損時に備えて、安全性の確保をするものです。



×勘違い2 「同期(ミラーリング)ツールを使っている」からOK!

「同期」は「鏡」です。
元データが壊れたり
ウイルス感染したりすると、
同期先も即座に「壊れた状態」に
更新されます。
「昨日の正常な状態」には戻せません。



×勘違い3 USBメモリに手動コピー

人間は忘れる生き物です。手動運用は必ず形骸化します。
また、USBメモリは紛失リスクが高く、長期保存にも向きません。



③【解決策】物理とクラウド、どう使い分ける？

正しいバックアップのためには、「物理(オンプレミス)」と「クラウド」、それぞれの特性を理解し、両方使う(ハイブリッド)のが現代の正解です。

① 物理バックアップ(NAS・バックアップサーバー)

社内にバックアップ専用の機器を置く方法です。

メリット	復旧が速い	社内ネットワーク内にあるため、大容量データでも短時間で戻せます。
	コスト	機器購入の初期費用のみで、月額費用がかからない場合が多いです。
デメリット	災害に弱い	オフィスが火事や地震、泥棒被害に遭うと、データも一緒に失われます。
	故障リスク	機械なので、数年で壊れる可能性があります。

② クラウドバックアップ

インターネット上のデータセンターにデータを保存する方法です。

メリット	災害に最強(BCP対策)	オフィスが物理的に消滅しても、データは安全な場所に残ります。
	ランサムウェアに強い	多くのサービスが、ウイルスが書き換えられない仕組みを持っています。
デメリット	復旧に時間がかかる	インターネット経由で戻すため、TB単位のデータだと数日かかることもあります。
	コスト	毎月の利用料(サブスクリプション)がかかります。

③【推奨】「ハイブリッド・バックアップ」でさらに強化する。

どちらか一つではなく、両方を組み合わせることで、お互いの弱点を補完します。

最強の運用イメージ

① 1次バックアップ(物理)

社内のバックアップ用NASやHDDに、毎日自動でバックアップ。

目的 「誤って消した」「ファイルが壊れた」など、日常のトラブルから「数分で」復旧するため。

② 2次バックアップ(クラウド)

物理バックアップのデータを、夜間に自動でクラウドへ転送。

目的 「火災」「地震」「ランサムウェアで全滅」などの壊滅的被害から、「確実に」会社を再建するため。

④ バックアップのポイントを簡潔に整理します。

① いつ取るか(取り方)

オフライン	システムを止めて取る(夜間など)。確実だが、その間使えない。
オンライン	動かしたまま取る。止めずに済むが、重くなる可能性がある(システムによっては手順が必要)。
バックアップウィンドウ	バックアップしてよい時間帯(業務に影響が少ない時間)を決めること。

② 何を取るか(単位)

ファイル単位	必要なファイルだけ守る。一部だけ戻しやすいが、環境までは戻らない。
イメージ単位	PC/サーバーを丸ごと守る。復旧が早いですが、容量が大きい。機器が違えば戻しにくいことも。

③ どう残すか(世代の種類)

フル	毎回ぜんぶ。戻すのは簡単／時間と容量が大きい。
差分	前回フルからの変更。戻すのは比較的簡単／日が経つと増える。
増分	前回からの変更だけ。普段軽い／戻すのに手間、途中が壊れると弱い。
永久増分	最初フル＋あとは増分続ける。効率的だが仕組みが必要。

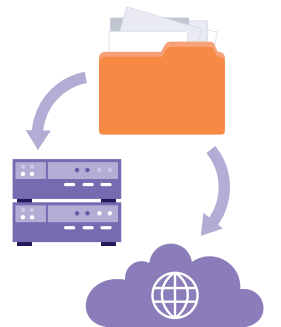
④ どこに置くか(保存先)

テープ	長期保管に向いている。切り離して保管でき攻撃に強いが、復元は手間。
ディスク(HDD/NAS)	速く戻しやすいが、同じ場所だと災害に弱い。管理も必要。ディスク(メモリー)でもUSBやポータブルHDDは危険!
クラウド	手軽で遠隔地に置いて災害に強い。ただし回線次第で遅い・設定(権限など)が大事。

⑤ 正しいバックアップの鉄則「3-2-1ルール」

どんなソフトや機器を使うにしても、このルールを満たしているか確認してください。

ルール	内容	意味・目的
3	データを3つ持つ	[1.元データ] + [2.物理バックアップ] + [3.クラウドバックアップ]
2	2種類のメディア	機器の同時故障を防ぐため、NASとクラウドなど異なる媒体を使う。
1	1つは遠隔地へ	これがクラウドの役割です。災害対策(BCP)になります。



⑥ 最後に:バックアップは「保険」です。

「バックアップが成功しました」というログを見て安心しないでください。
リストア(復元)テストを必ず実施してください



これらは本当によくある話です。

半年に一度は、「実際にファイルを1つ復元してみる」「災害を想定してクラウドからデータを戻してみる」訓練を行ってください。

まとめますね!有効なバックアップの要点は5つです。

- 1.自動で定期実行し、結果(ログ)を確認する
- 2.保存先を分ける(同じPC内に置かない。外付け/NAS/クラウド/遠隔地を併用)
- 3.履歴(世代)を残す(削除前・感染前などに戻せるように)
- 4.復元できるか定期的にテストする(手順も文書化)
- 5.バックアップ自体を守る(権限最小化、切り離し保管等で改ざん・暗号化を防ぐ)

企業の最重要資産である「データ」は、お金以上の価値、そしてお金では買い戻せない、企業にとって最も重要な資産です。正しく、確実にバックアップしましょう!



当社がしっかりご提案、
導入サポートいたします!

まっ
と
当社にご相談ください!

