

Acronis

#CyberFit



ディザスタリカバリ導入の 秘密の近道

目次

ディザスタリカバリ（DR）とは

貴社は準備ができていますか？

ITだけの問題ではありません

現実

脅威

進化したディザスタリカバリ

DRに投資すべき10の理由

ダウンタイムのコストを把握する

DRプログラムへの道筋

ビジネスの継続がかつてないほど簡単に

3

4

5

6

7

8

9

11

12

13

はじめに

バックアップを取れば十分、とお考えかもしれません。貴社のデータ、システム、アプリケーションが侵害を受けるまで、その本当の重要性に気付くことは難しいでしょう。ディザスタリカバリは、何らかの原因でシステムが停止した場合に、迅速に復旧するために不可欠なステップです。実際に、そのような事故が発生する可能性は低いかもしれませんが、いざという時にとても助かるものです。

ディザスタリカバリ（DR）とは

ディザスタリカバリ（DR）には、バックアップが必要です。DRは、システム全体の最新データのコピーとコンピューティング処理能力が含まれ、貴社の重要なデータ、システム、およびアプリケーションの復旧を自動化します。

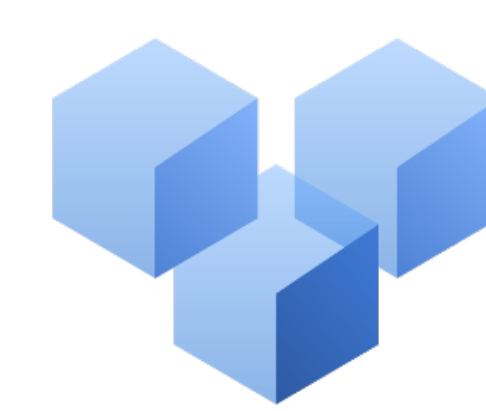
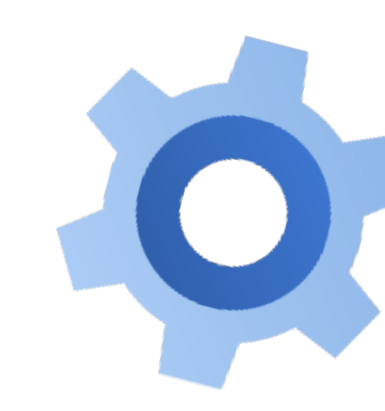
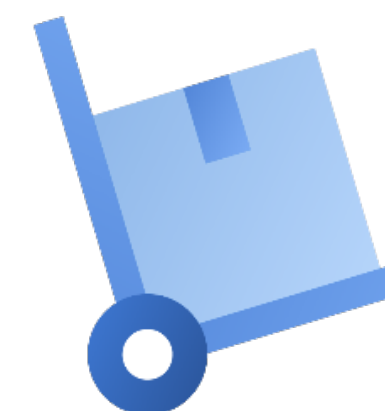
これにより、相互依存のプロセスを適切な順序で復元し、適切な復元ポイントに適切なタイミングで復旧することができます。

貴社は準備ができていますか？

DRaaS が必要なのは？ ビジネスを行うすべての事業者です。災害（ディザスタ）はいつやって来るかわかりません。あなたのビジネスは、自然災害が発生しやすい場所に位置していたり、技術的なリソースが不足していたり、ディザスタリカバリを実行するための経験が欠けている可能性があります。

次のような業界は、ミッションクリティカルなアプリケーションやデータに依存していたり、規制およびコンプライアンス違反で大きな罰金やペナルティが科せられるリスクがあります。

- 金融サービス
- 医療・ヘルスケア
- 法律
- 運輸
- 通信
- 製造
- 建設
- エネルギー
- eコマース（オンラインビジネス）
- 公益事業
- サプライチェーン/物流



ITだけの問題ではありません

ビジネスを平常に早急に復旧させることは、ITだけの課題ではありません。ITシステムの停止が、ヒューマンリソース、財務、法務、その他の部門に影響を及ぼすと、それは企業全体の問題となります。



IT

- バックアップと復元
- SLA（社内外）
- 従業員の満足度
- 監査
- コンプライアンスと規制



経営陣

- ビジネス継続性計画
- 市場認識
- 従業員の生産性
- コンプライアンスと規制
- 保険



財務

- コンプライアンスと規制
- 機密データの保護
- 事業運営の維持
- 市場および経済的信頼
- 監査



ヒューマンリソース

- 人材・労働力の計画
- トレーニング
- 従業員の生産性
- 機密データの保護



法律

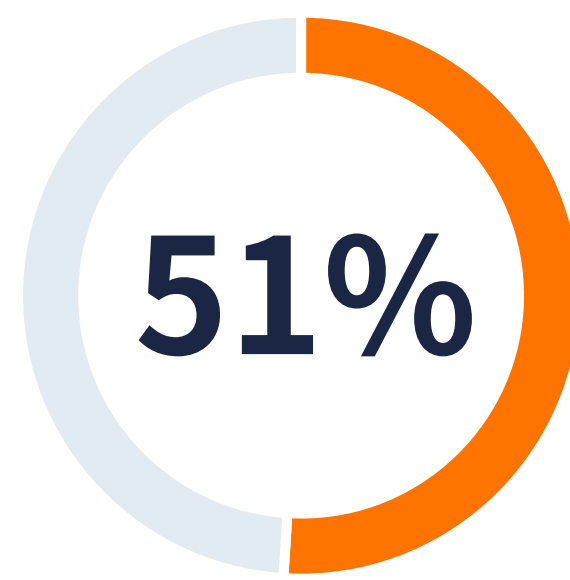
- コンプライアンスと規制
- 機密データの保護
- 保険

現実

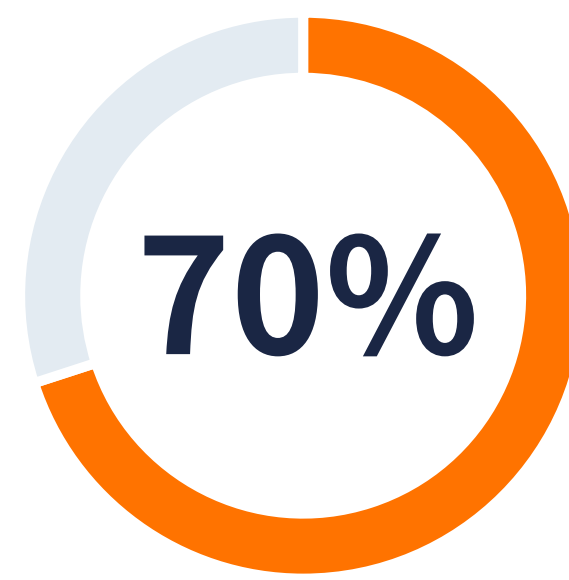
災害はいつでも、様々な形で起こりうるものです。貴社が迅速に事業を復旧できるよう、アクロニスがお手伝いします。



のデータ侵害（2019年）は、誤ってファイルやフォルダを削除したり、上書きしたことによるもの¹



のデータ侵害（2019年）は、犯罪および悪意ある攻撃によるもの¹



の組織は、復元不可能なデータ損失により、2022年までにビジネスの中断を経験する²



の事業者が過去3年以内に攻撃を経験³

2.2日

平均の
ダウンタイム²

5,600米ドル

平均の
1分間あたりのコスト²

392万米ドル

データ侵害によるコスト
総額の平均²

1) Ponemon Institute 社（2019年）。2) Gartner 社（2019年）。3) IDC 社（2019年）。

脅威

もしかすると、ハードウェアに影響する停電や、自然災害だけがダウンタイムにつながって考えていませんか？

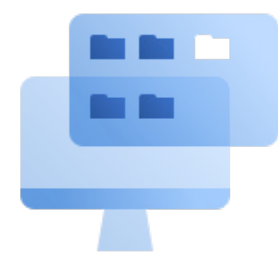
ソフトウェアや従業員が原因となるケースについても考慮する必要があります。テクノロジーが進歩するにつれて、社内、社外の脅威も増します。



自然災害

台風、水害、地震、火災は、施設やインフラに大きな影響を与え、深刻なダウンタイムにつながり兼ねません。

ただ、多くの企業が知らないのは、停電件数の6%のみが自然災害によるものだということです。



感染症の拡大

新型コロナなどの感染症の拡大は、組織の従業員に影響します。リモートワークの場合は、IT部門がこれまで想定していなかったような計画の必要性が次々と出てきます。

ITの通常の管轄外にデータやデバイスが持ち出されると、リスクが一気に上昇します。



ハードウェア障害とソフトウェアの破損

ハードウェア障害は、停電によって引き起こされることがあります。ソフトウェアは、ソフトウェアアップデートの失敗やドライブの不適切なフォーマットにより、正常に機能しないことがあります。



人的エラー

人間にミスはつきものです。ほとんどの人が、一度は、誤ってファイルを削除したり、上書きした経験があるでしょう。

不満を抱えた従業員がデータやシステムを破壊することもあります。



サイバー攻撃

一人の従業員のパソコンが侵害を受けたら、ネットワーク全体が脆弱になる可能性があります。

弱いパスワードや、フィッシングにひっかかったり、悪意あるリンクをクリックすることで、すぐに攻撃される可能性があります。

進化したディザスタリカバリ



企業のデータセンター (コロケーションage)

- 償却済みのハードウェア
- ネットワーク
- ライセンス
- レプリケーションプラットフォーム
- 膨大なストレージ容量



ハイブリッドアプローチ

- 高額ライセンス
- 複雑化
- 制限のあるストレージ



最新のハイブリッドおよびクラウドベースのDR

- 優れた費用対効果
- 使いやすい
- すぐに使える



DRに投資すべき10の理由

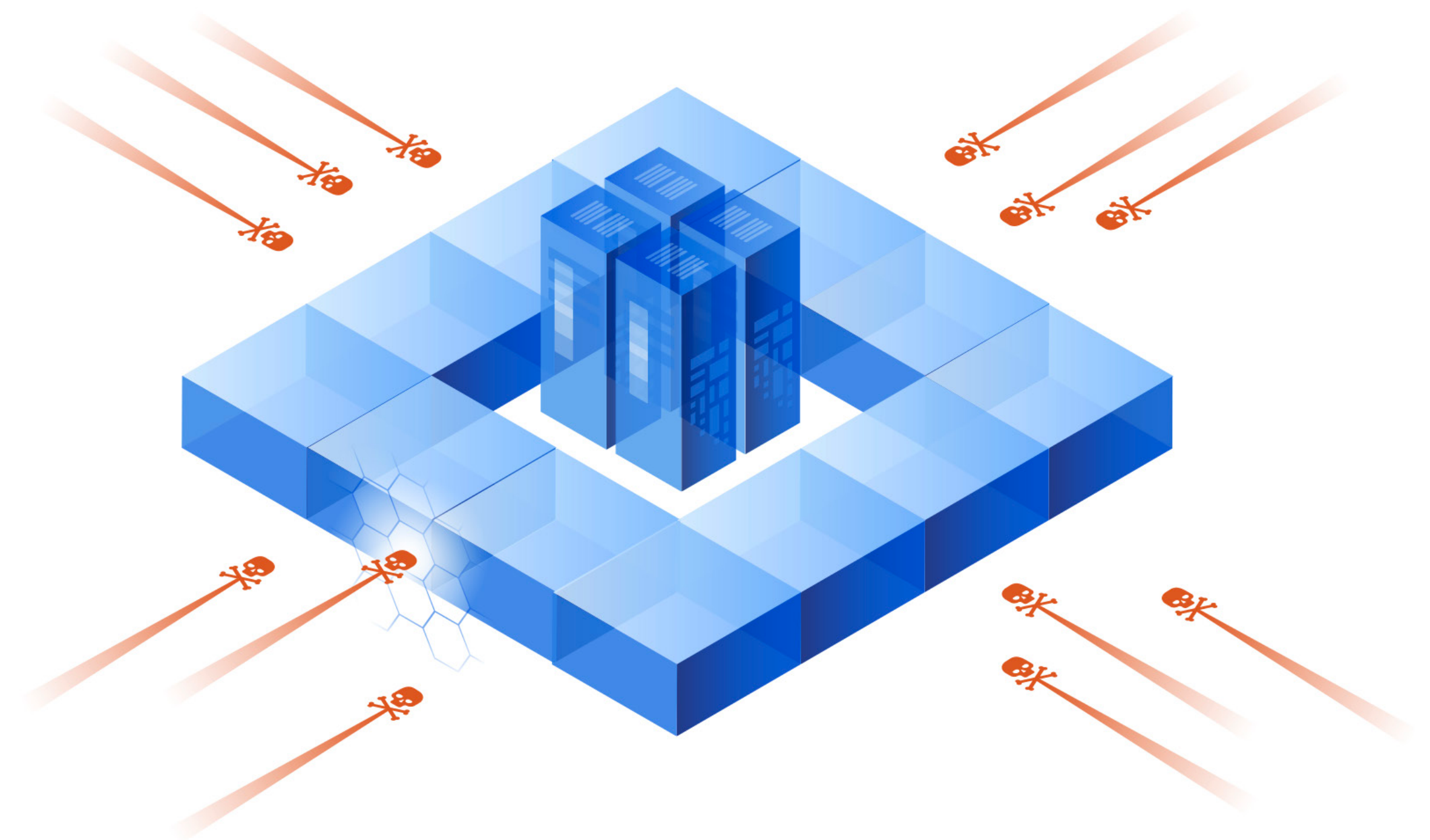
ディザスタリカバリを導入して、バックアップの一步先を目指すたくさんの理由があります。

- これまで以上に優れた費用対効果
- ディザスタの影響を最小化
- 継続的に従業員の生産性を維持
- コンプライアンスと規制の要件を遵守
- 即時復元を実現
- 事業運営のダウンタイムを軽減
- 潜在的な損失を低減
- 賠償責任のリスク低減
- 負の連鎖のリスク最小化
- 危機管理の促進



組織のシステムとデータに影響を与える様々な社内、および社外の要素を考えると...

実際、問題はデータ損失を経験するかどうかではなく、いつ遭遇するかです。



ダウンタイムのコストを把握する

これらの要素は、貴社の事業に合わせて考慮します。すべての部門のコストと統計を反映させて、実際の1時間当たりのダウンタイムコストを算出します。つまり、ダウンタイムは大きな損失につながる可能性があるということです。

収益の損失 + 生産性の低下 + 復旧にかかるコスト + 無形のコスト = **ダウンタイムコスト（1時間あたり）**

収益の損失

これは分かりやすいですね。ビジネスが中断されている間は、収益を生むことができません。

年間総売上高を基に、各事業領域でダウンタイム中に生じる、1時間あたりの収益の損失を算出します。

生産性の低下

従業員が業務を行えない、もしくは、収益に直結しない業務を行う必要性が生じても、ダウンタイムのコストは増加します。

給与や時給は固定費であり、従業員の生産性に関わらず、支払わなければいけません。

復旧にかかるコスト

多くの場合、復旧にかかるコストと、通常 of 事業運営を再開するためのコストを考えていません。

- 失われたデータを復元するためのサービスと従業員の時間
- 修理または交換が必要になる物理的なツールとデバイス
- データの損失によるコスト

無形のコスト

ブランドの風評被害は収益の損失につながります。ほんのわずかなダウンタイムでも、ビジネスにとって大きな打撃となる可能性があります。また、そのダウンタイムにどのように対処するかにより、復旧できるか、倒産となってしまうかの分かれ道となります。

DRプログラムへの道筋

自社のディザスタリカバリプログラムを管理するにあたって、次の要素が必要になります。

- 次のタスクに対応する人材
 - 評価
 - 設計
 - テスト
 - 実装
 - 管理
- トレーニング
- 文書化
- レポート作成
- インフラストラクチャの復旧

アクロニスの認定パートナーを選ぶメリット

- 長年にわたるディザスタリカバリのノウハウ
- 迅速かつ簡単に実行できるディザスタリカバリサービス
- 継続的かつ効率的な提供方法
- 24時間年中無休のサポート
- シンプルなテスト機能
- 監視および管理
- 統合されたクラウドストレージとコンピュートリソース
- 費用対効果に優れた運用コスト



ビジネスの継続はかつてないほど簡単に

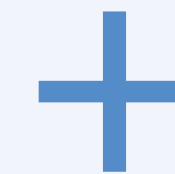
必要なのは、1つのエージェント、1つのコンソール、1つのクラウド。



データ保護



サイバーセキュ
リティ



ディザスタリカ
バリ

バックアップと復元

主なポイント

- 価値のあるデータの損失を回避
- サーバー、ワークステーション、モバイルデバイスに保存されたデータ

エンドポイント管理とセキュリティ

主なポイント

- マルウェアの攻撃の検出と遮断
- 脆弱性診断と構成管理
- URL フィルタリング
- パッチ管理

ディザスタリカバリ

主なポイント

- クリティカルなアプリケーションの
高可用性
- 迅速な復元でダウンタイムの
コストを低減

Acronis

#CyberFit



ありがとうございました

アクロニスが提供するディザスタリカバリのサポートについて、お気軽にお問い合わせください。

www.acronis.com | dr@acronis.com