Engineer

目標復旧時点

障害時に失ってもよいデータの期間の上限

どのようなものか

目標復旧時点とは、サービスが中断してデータを戻すとき、障害よりどれだけ前の状態までなら許容できるかを表す目標です。英語の頭文字からRPOとも呼びます。十五分と決めた場合、合意した障害の条件で、直前の十五分間までの変更は失ってもよいという意味です。検証できた最新の状態が五十分前なら、サービスをすぐに立ち上げられたとしても、データの目標は達成していません。

分数だけでなく、対象のデータと障害の想定を示します。信頼できる元の記録から作り直せるなら、ローカルなキャッシュを失っても影響が小さい場合があります。すでに利用者へ確定通知を出した注文を失う場合は、事情が異なります。一行を誤って消した場合と、地域全体が利用できない場合、資格情報が危険にさらされた場合では、使えるバックアップが異なることがあります。対象と条件を明確にすると、何を試せばよいかも分かります。

目標復旧時間で問題にするのは、機能が使えない状態がどれだけ続くかです。復旧時点では、どの状態が残ったかを見ます。毎日のバックアップは数分で復元できても、一日分の作業を失うかもしれません。最近の変更まで保持したコピーでも、検証や公開に長くかかることがあります。それぞれの目標を測ると、準備すべき作業の違いが分かります。

概念を判断に生かす

「目標復旧時点とは？」を実際の判断に生かしましょう。その概念を、開発または購入するシステムに結び付けて考えるお手伝いをします。 あると信じるだけでなく、復元を試したバックアップと、サーバーが起動しない朝に使える手順書を用意します。

サービスを見る お問い合わせ →

用語の背後にある前提を検証する

解説とリンク先の実績を参考に、プロジェクトについての質問を整理してください。ツールを選ぶ前に、前提を一緒に検討できます。 Barmanで重要データのバックアップ100件を自動化 — 100 データベース全体で自動化した重要バックアップ

Barmanで重要データのバックアップ100件を自動化 お問い合わせ →

なぜ重要なのか

バックアップの実行間隔は設計上の設定です。目標復旧時点は、結果として何を取り戻せるかの条件です。五分ごとに動くはずの処理が遅れたり、異常が報告されなかったり、ログを再適用できないコピーができたりすることがあります。時刻の分かる変更を置き、抜けのない状態をどこまで実際に復元できるかを確かめます。バックアップが成功した、というログだけでは見えない問題が分かります。

目標は、組織がどこまで記録を再構成できるかにも左右されます。失われた期間中に発行した領収書、受け付けた予約、取引先から届いた通知をどう扱うでしょうか。他の仕組みに耐久性のある記録があり、やり直せるものもあります。一つのアプリにしか記録がないものもあります。再構成の費用とリスクを調べ、担当者を決めます。重要な注文に厳しい目標を設けるほうが、キャッシュや報告書を含めてすべてに同じ数値を課すよりも役立つ場合があります。

コピーの頻度を上げるだけが方法ではありません。データに応じて、スナップショットと取引ログ、複製、変更できないコピー、別のシステムでのイベントの保管を組み合わせられます。何が残るかは障害で変わります。複製先は正当な変更も誤って削除した結果もすぐ受け取ります。別に保存したコピーも、復旧を担当する人が必要なときに読み出し、意味を理解し、検証できて役立ちます。

実際の活用例

Engineer ApSは実際にバックアップを復元した事例を公開しています。サービスレベルには、支援の範囲や引き継ぎに関する説明があります。事例から、復元を実際に試したことが分かります。以下の時間や数値は、目標復旧時点の測り方を示すための仮定です。

ある店がデータベース障害に備え、確定した注文の目標復旧時点を十五分と定めたとします。店はデータベースのスナップショットを作り、取引の記録を別に保管しています。演習で14:00に主系統へのアクセスを止めます。前もって13:45の前後に時刻の分かる注文を入力します。取り消しと支払いの変更も含めてください。当番の担当者が実際に持つ権限で、隔離した環境にデータを復元します。検証できる最新の整合した状態を見つけます。

13:50までに起きたはずの変更がすべて含まれていれば、観察された損失の範囲は10分間です。この演習では、十五分の条件を満たします。13:58の注文が一件見えるだけでは、それより前の記録が欠けているときに二分の損失とは言えませ

ん。行の識別子や合計を照合し、注文を処理するために必要な関連データも確かめます。記録を保存し、残った期間内の注文にどう対応するかを決めます。利用可能な機能が戻った時刻は別に記録します。

次の演習では条件を変えます。通常の担当者が共有の管理システムを使えない状況を試したり、誤って削除した場合を想定してその直前の状態を選んだりします。それぞれの条件でどのコピーが利用できるかを確かめます。一つの演習で測った結果は、その条件での根拠です。依存先が異なる障害は、別の演習で確かめます。

問題が起きるところ

複製の遅れだけを見て、失うデータの範囲を把握したと思うことがあります。アプリは注文を一つの保管先に書き、添付ファイルを別の場所に置くかもしれません。それぞれの時刻が違えば、新しいデータベースから、失われたファイルが参照されます。実際の復元で関連する記録を含め、保管先の境界をまたいで整合性を確かめます。

使えない認証情報、記録されていない暗号鍵、保管場所を覚えている一人の担当者に、手順が依存している場合もあります。本番で許可される当番役に手順書を渡し、その権限で練習します。時間と利用できる機能のうち、どれがまだ仮定かを書きます。コピー探しにかかった時間は、別に設けた目標復旧時間にも関係します。

データの再構成が難しくなったら、目標を見直します。最初は紙の注文台帳を写しただけのアプリなら、一日分を戻せない場合も別の記録から回復できるかもしれません。そのアプリが正式な唯一の記録になれば、同じ日数でも影響は変わります。古い測定が新しい業務に当てはまると判断する前に、業務責任者と許容範囲を確認し、改めて試します。

参考資料

- NISTによる連邦情報システムの緊急時対応計画の指針 — 復旧目標の定義と事業継続計画への組み込み。
- AWS Well-Architectedによる災害復旧の計画 — 障害の想定と復旧目標。
- NIST用語集の目標復旧時点 — 時間で表した許容できるデータ損失。

用語集

実際の制約に合わせて選ぶ

デプロイの流れ、運用上のリスク、緊急対応の担当者をお知らせください。検査、復旧手段、明確な責任の所在を伴う変更の範囲を定められます。

料金を見る お問い合わせ →

用語を実務に結び付ける

「目標復旧時点とは？」がお客様の組織にどう当てはまるかをご相談ください。現在のシステムの具体例が一つあれば、話を始められます。

サービスを見る

welcome@engineer.company +45 50 10 61 84 デンマーク、コペンハーゲン

このページを持ち歩く

連絡先カード

心を込めて丁寧に制作： D.

CVR 45969703 · Tagensvej 105C, 3. th, 2200 København N

著作権 © 2025 – 現在 · Engineer ApS · すべての権利を留保します。

印刷元： https://engineer.company/ja/glossary/recovery-point-objective/