Engineer

目標復旧時間

障害の発生からサービスを再開するまでの目標時間

どのようなものか

目標復旧時間は、サービスが中断してから、合意した機能を再び使えるようにするまでの目標時間です。英語の頭文字からRTOとも呼ばれます。組織がその機能なしでどこまで待てるかを表します。測定できる目標には、時計を動かし始める出来事と、使えるようになった証拠の両方が必要です。警報が鳴った時点を始まりにすると、障害に気づくまでの時間を除いてしまいます。プロセスが動いた時点で終えると、利用者がまだ使えない状態を復旧済みと判断しかねません。

NISTの緊急時対応計画の指針は、システムの資源がどれほど長く使えなければ、依存する資源や業務に許容できない影響が現れるかを基準にします。目標は、事業への影響を評価する中で定めます。先に再開が必要な仕事を挙げ、逆算してその仕事を支えるシステムを確認します。データベースや認証が業務アプリより早く使える必要があるのは、そのためです。

目標復旧時点、つまりRPOは、どれほど前の状態に戻ることまで許容できるかを表します。二十分で再開できても、直前の四時間分の変更を失うことがあります。反対に、変更はすべて戻せても、サービスは半日使えないかもしれません。可用性の目標は、月内に成功した要求の割合など、一定期間の動作を測ります。一回ごとの復旧が時間内でも、何度も中断すればその月の停止許容範囲を超える場合があります。

概念を判断に生かす

「目標復旧時間とは？」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

必要な準備は時間によって変わります。午前中の停止を許容できるなら、新しい環境へバックアップを復元する手順を用意するだけでも間に合う場合があります。数分で使える必要があれば、あらかじめ環境を整え、自動で確認できるようにし、すぐ判断できる人を待機させることが必要かもしれません。時間を使うのはデータの移動だけではありません。検知、担当者への連絡、判断、依存先の準備、検証、トラフィックの再開も含まれます。

時間を決めると業務への影響を具体化できます。商品を閲覧できても支払いができない期間は、商品を見るだけの利用者と、店のどちらにも同じ影響を与えるわけではありません。一時的に手作業で代替しても、新しい注文が処理より早く届けば未処理分が積み上がります。時計が止まる時点で使える機能を定義しておきます。最低限の業務を再開する期限と、すべての機能や残務を回復する期限を分けることもできます。

目標は計画で、演習の結果は観察です。小さな試験環境でたまたま早く復元できても、サービス全体が同じ時間で戻るとは限りません。データ量、利用できた依存先、判断を担当した人、利用者を戻せるとした根拠を記録します。その条件が分かると、結果をどう解釈できるかが見えてきます。

実際の活用例

注文を受け付けて記録する機能を二時間以内に再開する、という目標を考えます。利用者が注文できなくなった時点から測ります。演習なら、障害を起こした時刻を記録しておけば、検知するまでの時間も含められます。代表的な注文が決済の確認に進み、倉庫が見る画面や記録に現れることを、使えるようになった条件とします。カタログが開けるだけではまだ止めません。

演習では、検知までに十二分かかりました。インシデントを宣言し、コピーを選んで復元を承認するまでに十八分、データを戻す作業に四十五分かかりました。依存先をつなぐ作業、試験の注文、利用再開にさらに三十分かかりました。所要時間は105分で、目標まで十五分の余裕がありました。データの損失については、復元した最も新しい注文の時刻を別に確かめます。

この結果は、使ったデータと依存先の条件に照らして判断します。接続のし直しに時間がかかったのなら、設定の一部を事前に用意できるかを見ます。交代の時間帯に承認する人が見つからなかった場合は、判断を任せる範囲を明確にします。後の演習では、現実的なデータ量と別の担当者を使い、同じ開始と終了の基準で比べます。再開後に照合する注文についても担当者を決めます。

Engineerのバックアップを復元して確かめた事例は、復元の確認を含む仕事を紹介しています。公開されているサービスレベルでは、対応の範囲や応答などの支援条件を説明しています。二時間という目標や上の各作業時間は、ここで考えた架空の注文サービスのための設定です。

問題が起きるところ

記録にある時刻を都合よく使う。 最初の復元操作から測ると、それまでに利用者が待った時間が消えます。停止、検知、操作をそれぞれ記録し、結果がどの区間に当たるかを書きます。

構成要素が起動しただけで復旧とする。 データベースが動いていても、支払いに失敗することがあります。代表的な利用の流れを試し、その結果が依存するシステムまで届くか確かめます。

すべてに同じ期限を割り当てる。 前の作業の完了を待たなければならない場合があります。依存関係を見て全体の時間に収め、判断や承認にかかる時間も見込みます。

試していない数値が約束になる。 遅れた試験や失敗した試験も含めて、目標と複数の結果を比べます。実施条件を残せば、一回の速い復旧をすべての障害に当てはめずに済みます。

参考資料

- NIST SP 800-34改訂第1版 — 緊急時対応計画、事業影響の分析、復旧目標。
- AWSによる復旧目標の指針 — 停止時間とデータ損失、それぞれの目標。
- Microsoft Azureによる事業継続と復旧の解説 — 可用性と復旧能力の違い。

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

「目標復旧時間とは？」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-time-objective/