Engineer

災害復旧

大きな損失の後、検証済みの計画でサービスを戻すこと

どのようなものか

災害復旧は、緊急時対応計画のうち、最悪の場合を扱う部分です。システムの稼働場所を失うか、長期間アクセスできなくなり、コピーを使って、別の場所にシステムを再構築する必要がある場合です。NISTの「連邦情報システムの緊急時対応計画ガイド」、2010年のSP 800-34改訂1は、災害復旧計画を、ハードウェアまたはソフトウェアの重大な障害、あるいは施設の破壊の後、一つ以上の情報システムを代替施設で復旧するための文書化した計画と定義します。対象範囲は限定されています。ガイドは、主要施設に長期間アクセスできなくなる重大な中断、通常は物理的要因による中断を対象とし、移転が必要な中断だけを扱います。

この範囲の狭さが、関連する計画との違いです。ガイドでいう情報システム緊急時対応計画は、ディスクの故障でも、データベースの破損でも、一つのシステムを、どこに置かれていても復旧します。災害復旧計画は、拠点に結び付いた計画です。業務を代替拠点へ移し、そこで各システムを、それぞれの緊急時対応計画に従って起動します。一つのデータベースの計画と、データセンター全体、クラウドのリージョン、プロバイダーのアカウントを失う場合の計画は、文書も責任者も異なります。両者を混同すると、企業は、どちらの計画も持たないままになってしまいます。

三つの尺度によって、計画は、意図の表明から検証できるものへ変わります。最大許容停止時間、MTDは、システムの責任者が受け入れる、停止の総時間です。目標復旧時間、RTOは、ほかのシステムや事業への損害が許容できなくなるまで、システムのリソースを利用できないままにしてよい最長時間です。中断した仕事は、その後に再処理する必要もあるため、ガイドは通常、RTOをMTDより短くする必要があるとしています。目標復旧時点、RPOは、過去に目を向けます。最新のバックアップからデータを戻せる、停止前の時点で、事業が許容できるデータ損失を表します。簡単に言えば、RTOは停止時間、RPOは失う仕事の量です。

代替拠点には、準備の程度による種類があります。コールドサイトは、場所とインフラだけを提供します。ウォームサイトは、一部の設備を備え、ホットサイトは、必要な設備と人員をすべて備えます。ガイドは、さらにモバイルサイトとミラーサイトを挙げます。モバイルサイトは、多くの場合、24時間以内に搬入でき、その後に設置を始めます。ミラーサイトは最も高価な選択肢で、ガイドは「事実上100パーセントの可用性」を持つとしています。コールドサイトの維持費は最も安いものの、設備をそろえるには、かなりの時間がかかる場合があります。現在のソフトウェアの多くでは、第二のクラウドリージョンや別のプロバイダーが、同じ役割を担います。何を準備しておくかと、その維持費の兼ね合いも同じです。

概念を判断に生かす

「災害復旧とは？」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

バックアップはコピーで、コピーだけでは何も動きません。コピーから稼働するシステムへ戻すには、読み取るソフトウェア、復号する鍵、実行するサーバーとネットワーク、それらを結ぶ設定、作業の順序を知る人も必要です。失った拠点にしかなかったものは、どれも一緒に失われます。災害復旧は、すべてが同じ出来事を生き延び、必要になる前に、コピーからサービスまでの経路を実際にたどってある状態を整える取り組みです。

バックアップの予定がどのRPOを目指していても、復元できるデータの新しさは、実際に復元できる最新のコピーまでです。毎晩のジョブが一週間、何も知らせずに失敗していれば、方針文書に何とあっても、一週間分のデータが失われるおそれがあります。NISTのガイドは、テープでも同じ点を指摘します。データを正しく保存し、ファイルをエラーも損失もなく取り出せることを確かめるため、定期的にバックアップをテストするよう勧めています。バックアップジョブの緑の表示が証明するのは、何かを書き込んだことです。読み戻せることを証明するのは、復元だけです。

計画も古くなります。人は去り、サーバーは交換され、プロバイダーの管理画面は変わり、手順書のパスワードは期限切れになります。NISTが示す緊急時対応計画の七段階で、最後の二つは、テスト・訓練・演習と、計画の保守です。ガイドは、少なくとも年一回、またシステムや復旧に使うリソースが大きく変わるたびに見直す、生きた文書を求めています。一度も演習していない計画は、書くことを誰も思い付かなかった細部で失敗しがちです。サービスを起動する順序、有効期間が一日のDNSレコード、失ったマシンだけに保存していた唯一の認証情報などです。

ソフトウェアチームでは、建物よりも、アカウントが災害の対象になることが多くあります。削除されたクラウドプロジェクト、侵害された管理者ログイン、停止されたプロバイダーのアカウント、本番に対して実行した破壊的なコマンドは、洪水と同じように、システムへのアクセスを完全に奪います。最後の場合、スタンバイサーバーでは防げません。ほかの変更と同じように、誤った `DROP TABLE` も、すぐに適用してしまうためです。

実際の活用例

PostgreSQLのデータベースでは、ベースバックアップに加え、先行書き込みログ、WALを継続的にアーカイブすることで、二回のバックアップの間隔よりも、はるかに短いデータ損失期間に対応する復旧時点を得られます。サーバーは、完成したWALセグメントを安全な場所へコピーします。復元時には、ベースバックアップへそれらを再生し、取得後の任意の時点まで進めます。

```
# 保護対象のサーバー上のpostgresql.conf
wal_level = replica
archive_mode = on
archive_command = 'test ! -f /mnt/archive/%f && cp %p /mnt/archive/%f'
```

復元するには、新しいデータディレクトリーにベースバックアップを展開し、`recovery.signal` という空のファイルを置きます。復旧設定には、アーカイブの場所と、停止する時点を指定します。

```
restore_command = 'cp /mnt/archive/%f %p'
recovery_target_time = '2026-03-10 17:14:00+01'
recovery_target_action = 'pause'
```

PostgreSQLの文書は、これらの設定が必要になる例を示しています。火曜の夕方5:15に重要なテーブルを削除し、水曜の正午に気付いて、5:14まで戻す例です。目標に達すると、既定では一時停止します。接続を受け付けるためにサーバーを昇格する前に、クエリーで、正しい時点か確かめられるようにするためです。違う場合は、サーバーを停止し、後の時点を指定して、再起動します。選ぶ復旧時点は、ベースバックアップが完了した後でなければなりません。また文書は、最初のベースバックアップの前に、アーカイブを設定し、テストするよう勧めています。復旧が完了すると、サーバーは `recovery.signal` を削除し、誤って再び復旧へ入らないようにします。

Engineer ApSは、バックアップと災害復旧をサービスとして提供しています。バックアップを、できているはずと考えずにテストし、サーバーが復帰しない朝のために、計画を文書にするサービスです。ポートフォリオの二つのページが、その意味を示します。2025年からの職務で手がけたコードによるバックアップと災害復旧では、Bicepで、データベースと並べてバックアップの保持設定を定義しました。そのため、特定時点への復元は、誰かが一度ポータルでクリックした設定ではなく、テンプレートの一部です。データベースを取り巻く環境も、コードで定義しました。記憶に頼って再構築した環境へデータベースだけを戻しても、復旧したとは言い難いためです。その後、復旧への備えを監査し、不足点を明記して文書化しました。地理冗長性は無効で、演習を実施していないため、目標復旧時間は測定値ではなく、提案でした。

自社のバックアップと復元テストの自動化は、プロバイダーのスナップショットだけに頼らない復旧を目指して設計しました。Ansibleのロールが、resticのスクリプトとsystemdのユニットをインストールします。設定がある場合のデータベースダンプ、SFTPによる別プロバイダーのストレージへの暗号化・重複排除済みスナップショット、保持方針に従った削除、整合性検査を扱います。別の月次ワークフローは、既知のファイルを一時的な場所へ復元し、バイト列を照合します。バックアップと復元の成功シグナルは別で、パスフレーズは保護されたファイルから読み、タイマーは設定済みのリポジトリに依存します。これらの制御は実装済みですが、実環境での復旧は別の納品事項です。2026-10-27付の実装記録は、リポジトリがないためタイマーを無効にしていたとし、実環境での復元完了を記録していません。裏付けるのは自動化の実装であり、復旧時間の約束や、すでにホストの喪失に安全に対応できるという主張ではありません。

問題が起きるところ

バックアップを、一度も復元していません。 毎晩成功を報告するジョブだけでは、その出力を読み、復号し、読み込めるかは分かりません。初めて実際に復元するときに、読み込めるかを確かめるのは適切ではありません。バックアップと

同じように、復元も予定します。既知のデータを取り出して照合する自動検査と、クリーンな環境への完全な復元を行います。所要時間が実測値になる頻度で、繰り返します。

コピーが、元と同じ運命をたどります。 同じクラウドアカウントのスナップショット、同じラックのバックアップディスク、同じ管理者ログインの先にあるアーカイブバケットは、本体を失わせる出来事によって、一緒に失われます。NISTのガイドは、拠点外のストレージと代替拠点を、同じ災害に遭う可能性の低さで選ぶよう求めています。別のプロバイダー、または認証情報を分けた別のアカウントに、少なくとも一つのコピーを置きます。復号鍵も、保護するシステムに依存しない場所へ保管します。

データの復元だけを、計画しています。 サーバー、ファイアウォール規則、DNS、証明書、シークレットを記憶から作り直すなら、データベースの復元は、サービス復旧のごく一部です。バージョン管理するインフラコードで環境を定義し、演習には、データの読み込みだけでなく、環境の再構築も含めます。

目標が、推測です。 演習の裏付けなしに文書へ書いたRTOは提案で、すべてのバックアップが成功したと仮定するRPOは楽観的です。演習で、両方を測ります。NISTは、話し合いだけで機器を展開しない机上演習と、業務を模擬する機能演習を分けています。後者には、計画のすべての要素を扱う全面的な演習まで含みます。数字が得られるのは、後者です。

スタンバイを、バックアップとして扱います。 スタンバイサーバーや地理的に離れた場所へ複製したデータベースは、ハードウェアを失う事態への備えになります。しかし、正しい書き込みと同じ忠実さで、削除、破損、ランサムウェアが暗号化したファイルも複製します。本体の間違いが届かない、過去の時点のコピーを保持します。通常、間違いに気付くまでの期間よりも、長く残します。

計画が、昨年のシステムを説明しています。 廃止したサーバー、すでにいない担当者、使えないパスワードを並べた手順書は、復旧を導くどころか、遅くします。大きな変更の後と、演習の後に、計画を見直し、演習でうまくいかなかった点を記録します。NISTも勧めるように、連絡先の一覧など、変化の多い部分は、さらに頻繁に見直します。

参考資料

- SP 800-34改訂1：連邦情報システムの緊急時対応計画ガイド — DRPの定義と範囲、七つの計画段階、MTD、RTO、RPO、代替拠点、演習の種類を扱うガイド全体です。計画のテンプレートも含みます。
- 継続的アーカイブと特定時点への復旧（PITR） — WALのアーカイブ、ベースバックアップ、選んだ時点への復元を扱う、PostgreSQL 18の章です。
- 先行書き込みログ — `archive_command` 、 `restore_command` 、復旧目標の設定についての、構成リファレンスです。

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

「災害復旧とは？」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/disaster-recovery/