PostgreSQL インサイド

PostgreSQL の災害対策

地震や豪雨からデータを守る災害対策

技術を知る

FUJITSU

☐ 導入／環境設定　☐ 移行　☐ 性能　☐ チューニング　☐ バックアップ／リカバリー

☐ 冗長化／負荷分散　☐ 監視　☐ データ連携　☑ 災害対策　豆知識

地震大国の日本では震災に加えて、近年の異常気象による豪雨災害も多発しています。こうした災害がビジネスに与える脅威と損害は計り知れません。また、情報システムの長期の停止は、ビジネスの損失だけでなく、社会に与える影響も大きいため、遠隔地に災害対策システム（災害対策センター）を構築することがとても重要となっています。

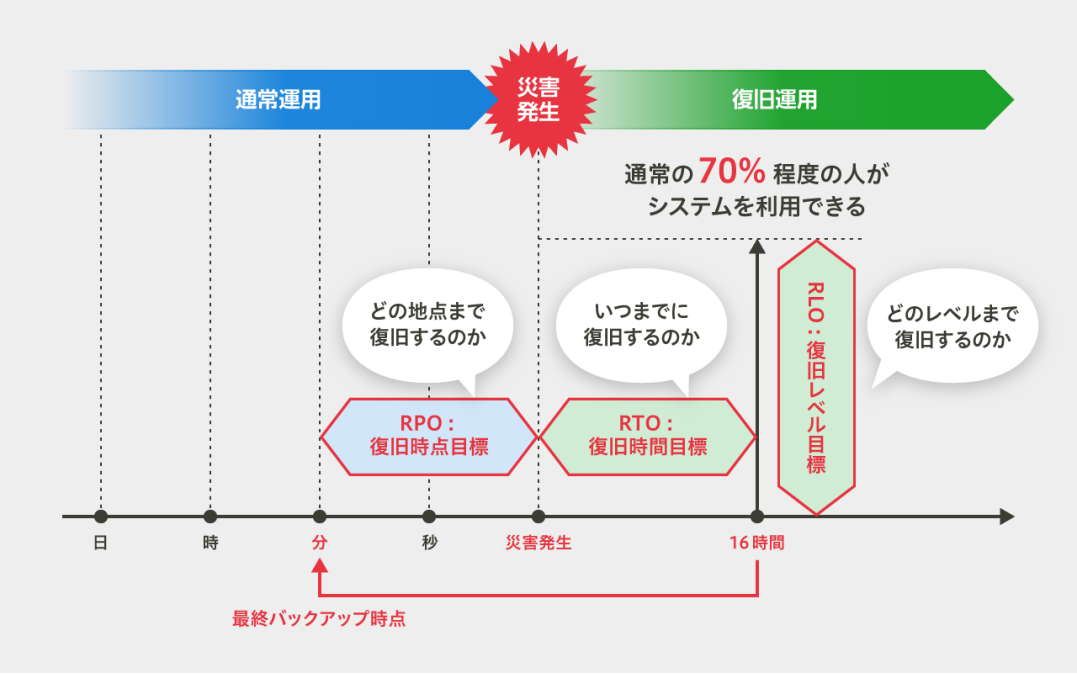
ここでは、PostgreSQL により、広域災害からデータベースを守る「災害対策」について解説します。

1. 災害対策を考える上で重要な「3 つの指標」

災害対策では、「災害からシステム（データ）を守る」ことはもちろんですが、「災害などの不測の事態が起きてもシステムが停止しない」「システムが停止した場合には、効率よく・迅速にシステムを復旧し、いつも通りに稼働させる」という観点から、事業継続計画（BCP：Business Continuity Planning）を策定することが重要です。
業務継続に必要な資産には、ハードウェアやソフトウェアの物的資産、オペレーターやシステム管理者といった人的資産、そして、業務で利用するデータがあります。これらを考慮し、「いつまで（RTO）」、「どの時点まで（RPO）」、「どのレベルまで（RLO）」にシステムを復旧させるのかを考え、目標値を設定します。

RTO（復旧時間目標）	Recovery Time Objective の略です。 災害発生後、いつ（何時間後）までにシステムを復旧するかの目標値です。
RPO（復旧時点目標）	Recovery Point Objective の略です。 災害発生前の、どの時点（ポイント）までシステムまたはデータを復旧するかの目標値です。
RLO（復旧レベル目標）	Recovery Level Objective の略です。 災害発生後、システムの機能や性能をどのレベルまで復旧するのかの目標値です。

例えば、「災害発生後 16 時間以内に、災害発生 1 分以内の状態に復旧し、通常の 70%程度の人がシステムを利用できるレベルまで復旧させ、業務を再開する」と目標を設定した場合は、以下のようになります。

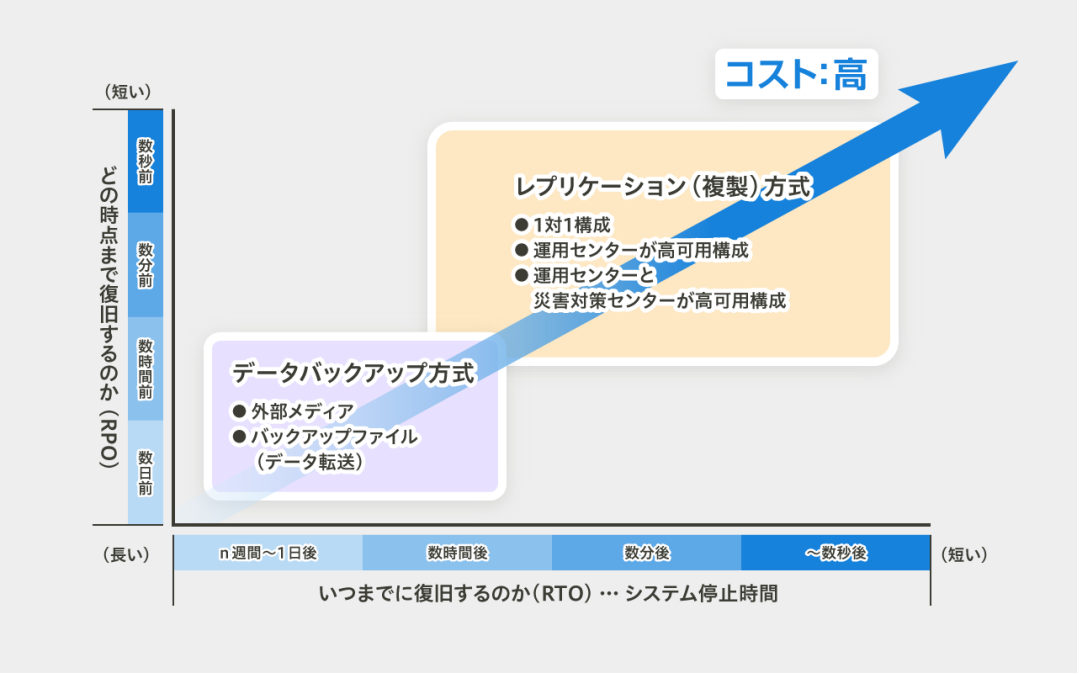


2. 復旧目標から災害対策を考察

データベースでは、「RTO」、「RPO」、「RLO」の観点で、どのような対策がとれるのか考えてみましょう。
データベースの遠隔地へのデータ転送方式には、「データバックアップ方式」と「レプリケーション（複製）方式」の 2 つがあります。「データバックアップ方式」は、運用中のデータベースのデータや定義ファイルをバックアップして遠隔地の拠点へ送り、災害時にそのデータを基にデータベースを再構築する方式です。一方、「レプリケーション方式」は、運用中のデータベース（システム）の複製を遠隔地の拠点に用意しておき、双方のデータベースで同じデータを保持することで、災害時には複製に切り替えて業務を継続 / 再開する方式です。

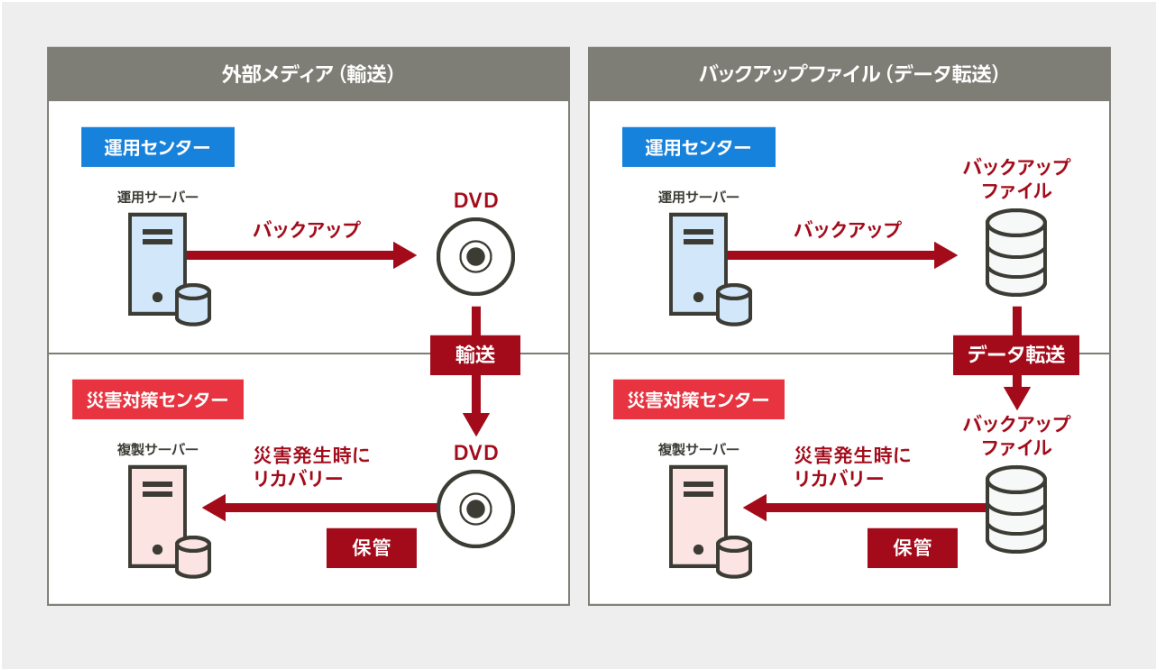
「RTO」は、システム停止やサービス中断が許される時間となります。RTO を短くするには、災害発生後、速やかにシステムの復旧作業に着手し、完了させることがポイントとなります。システムの復旧作業にかかる時間は、「データバックアップ方式」を採用しているか、「レプリケーション方式」を採用しているかで、大きく異なります。
「RPO」は、災害発生直前に戻すのか、何分前・何時間前の状態に戻すのかなど、どの時点まで復旧するのか、となります。例えば、金融機関で扱う数字データは最新性が重要なため、災害発生直前に戻す必要があります。この場合、データの更新に応じてバックアップを行う必要があるため、「レプリケーション方式」が適しています。逆に、更新頻度の低いデータや参照系システムのデータの場合は、損失するデータとコストの観点から、「データバックアップ方式」が適しています。
「RLO」は、サービスの範囲（レベル）、応答時間、接続数などを、いつまで（RTO）に、どのレベルに復旧したら業務を再開させるかの指標です。例えば、「災害発生後 16 時間以内に、通常の 70%程度の人がシステムを利用できるレベルまで復旧させ、業務を再開する」などの目標値です。RLO は RTO と合わせて決定する必要があります。

災害に備え RTO と RPO をより高い目標値に設定する場合、システムが継続して稼働できるよう、システムを高可用構成にすることが重要です。高可用構成にするには、運用センター側のハードウェア・ソフトウェア、災害対策センター側のハードウェア・ソフトウェア、また、それらを繋ぐネットワークの冗長化が必要になります。冗長化することにより、設備コストや構築 / 運用 / メンテナンスなどの人的コストがかかります。
そのため、RTO、RPO の設定で重要なことは、業務に応じた目標値を設定し、十分な事前設計をすることです。すべての目標値を高く設定することは理想ですが、コストが高くなりすぎないように、何を最優先とするか検討し、それぞれの目標値を設定し、それに適した災害対策システムを考えてください。



3. データバックアップ方式による災害対策

「データバックアップ方式」は、定期的にデータベースのバックアップを取得し、遠隔地の拠点へ送る方法です。
運用サーバーで定期的にデータを外部メディア（DVD やカートリッジテープなど）にバックアップし、それを遠隔地に輸送して保管することで、災害復旧時には、バックアップデータ取得時点にまで復旧することができます。また、データベースのバックアップファイルをそのまま遠隔地にデータ転送することで、バックアップデータ取得時点にまで復旧することができます。
バックアップした時点から、次回のバックアップまでの更新データは保持していないため、システムによってはデータの損失は多くなります。また、災害復旧時はデータベース全体をリストアするため、復旧時間が長くなります。しかし、通常実施するバックアップをそのまま災害対策にも生かせるため、災害対策を簡単に始められます。

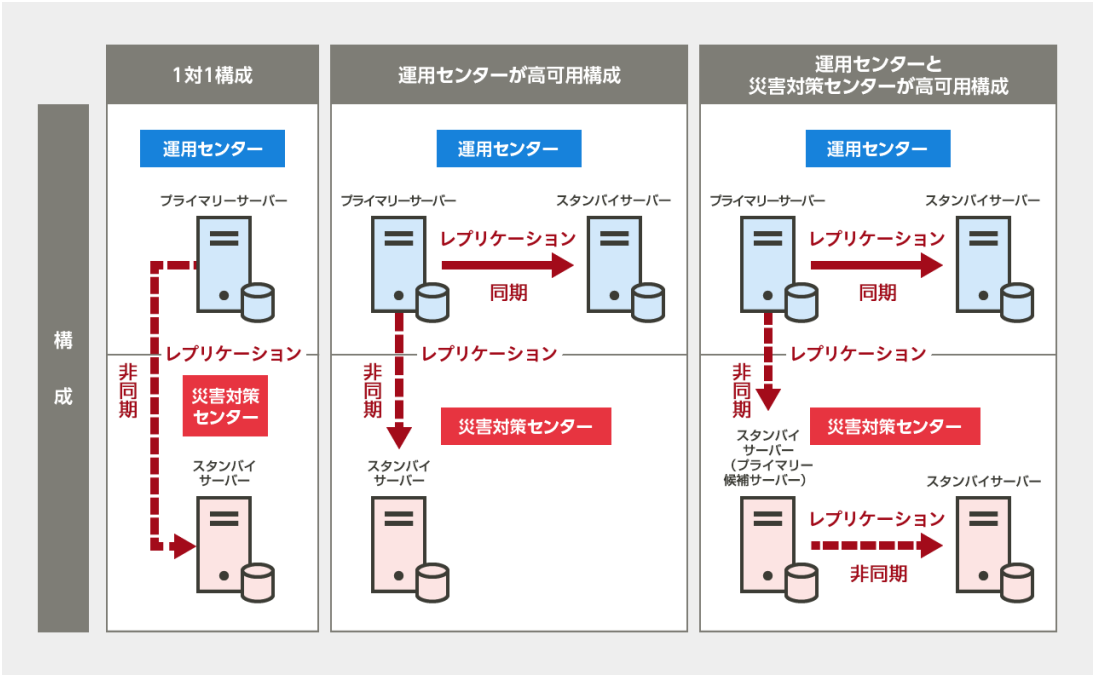


データバックアップ方式を PostgreSQL で実現するには、バックアップ・リカバリー機能を利用します。PostgreSQL の標準機能を利用するため、別途、災害対策用のソフトウェアを用意する必要はありません。バックアップ・リカバリー機能の詳細については、「技術を知る：PostgreSQL のバックアップとリカバリー」を参照してください。

4. レプリケーション方式による災害対策

「レプリケーション方式」は、運用センターのデータベースの更新ログを、災害対策センターのデータベースに反映する方法です。
データベース（システム）の複製を作成するため、常に双方のデータベースで同じデータを保持することができます。随時、更新ログを転送・反映しているため、災害時のデータの損失は少なく済みます。また、災害復旧時は、センターを切り替えるだけで業務を継続することができます。しかし、運用センターまたは災害対策センターで常時稼働するためのハードウェアが追加で必要となり、コストが高くなります。また、システム構築、運用手順、監視、トラブル対応の手順が複雑になるため、災害対策の運用を開始するまでに多くの時間が必要となります。
レプリケーション方式で実現可能な災害対策の構成には、以下の 3 つがあります。災害発生後や障害発生後の信頼性、ハードウェアや人的コストの観点から、適した構成を選択してください。

1 対 1 構成	双方のデータベースで同じデータを保持しているため、データの損失が少なく済みます。また、災害復旧時は、センターを切り替えるだけで業務を継続することができます。
運用センターが高可用構成	上記に加え、運用センターを二重化することで、運用センター内で障害が発生した場合にも信頼性の高いシステムを実現することができます。
運用センターと災害対策センターが高可用構成	上記に加え、災害対策センターも二重化することで、広域災害に備えた信頼性の高いシステムを実現することができます。被災により運用センターを切り替えた後も、被災前と同等の構成で業務を継続することができます。



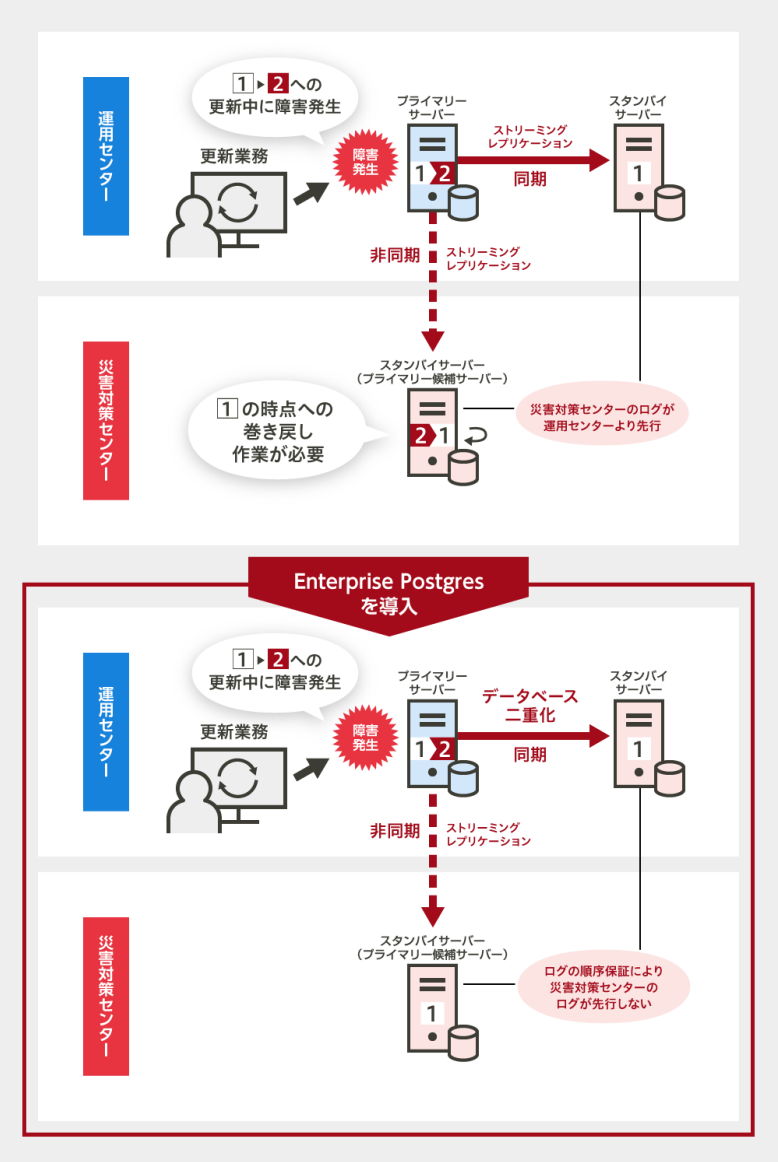
レプリケーション方式を PostgreSQL で実現するには、ストリーミングレプリケーション機能を利用します。PostgreSQL の標準機能を利用するため、別途、災害対策用のソフトウェアを用意する必要はありません。
ストリーミングレプリケーション機能は、データベース全体をレプリケーション（複製）するので、簡単かつシンプルに複製を作成することができます。また、ストリーミングレプリケーション機能は「同期」と「非同期」を選択することができ、例え

ば、運用センター内の冗長化には「同期」を、災害対策センターとのレプリケーションには「非同期」を、とストリーミングレプリケーション機能だけで対応することができます。

FUJITSU Software Enterprise Postgres でより安全な災害対策を実現

PostgreSQL のストリーミングレプリケーション機能で運用センターを高可用構成にした場合、運用センターのプライマリーサーバーからスタンバイサーバーにログを同期する一方で、災害対策センターのスタンバイサーバー（プライマリー候補サーバー）に非同期でログを送信します。この 2 つが連動していないため、ネットワークやサーバーの負荷の関係で、運用センターのスタンバイサーバーへのログ送信が遅延した場合、災害対策センターへのログ送信が先行してしまう可能性があります。このような状況下で、運用センターのプライマリーサーバーで障害が発生し、スタンバイサーバーに切り替えを行うと、災害対策センターへのログ送信を停止し、災害対策センターを運用センターのプライマリーサーバーと同等の状態に巻き戻さなければなりません。災害対策センターが停止すること自体が好ましくないうえに、この巻き戻し中に災害が発生した場合、せっかく用意した災害対策センターを即時活用できないという課題があります。

FUJITSU Software Enterprise Postgres（以降、Enterprise Postgres と略します）は、PostgreSQL のストリーミングレプリケーション機能による災害対策センターへのログ送信が先行しないよう、運用センターのスタンバイサーバーへのログ送信が完了したあと、災害対策センターへログを送信します。運用センターのスタンバイサーバーへのログ送信と災害対策センターへのログ送信の順序性を保証することにより、災害対策センターの運用一時停止や巻き戻し作業が不要となります。別途、Enterprise Postgres を用意する必要はありますが、ログ送信の順序性を保証することで、常時から信頼性を高めることができます。



ここでは PostgreSQL と Enterprise Postgres の災害対策を解説しました。PostgreSQL のストリーミングレプリケーション機能や Enterprise Postgres を活用し、地震や豪雨からデータを守る災害対策を検討してください。

2019 年 2 月 4 日