

Symfowareディザスタリカバリ

Symfoware Disaster Recovery

あらまし

企業情報システムの安定稼働に対するニーズは、年々高まっており、近年では、とくに自然災害やテロなどの災害に向けた対策が急務となっている。

Symfowareは、お客様にゆるぎない安心を提供している高信頼なデータベースであり、災害時にも安定稼働に向けた最適なソリューションを提供する。例えば、広域災害が発生しても、遠隔地に待機センタを準備しておき、センタを切り替えることでお客様のデータを守り、迅速な業務再開を実現する。

本稿では、メインフレームの実績技術やハードウェア新技術など富士通のコアコンピタンスを集結したSymfowareディザスタリカバリを説明する。

Abstract

The demands for stable operation of corporate information systems continue to grow, and in recent years, there has been an urgent demand for protection against natural disasters, terrorisms, and other destabilizing events. To meet these demands, Fujitsu offers its Symfoware Disaster Recovery system, which is based on the Symfoware high-reliability database and incorporates Fujitsu's expertise in mainframes, new hardware, and other core technology areas. When a disaster occurs at a customer's main center, this system switches operation to a previously prepared remote standby center. By using this system, customers can protect their data and quickly resume business activities when a disaster occurs. This paper describes the Symfoware Disaster Recovery system.



山口正人(やまぐち まさと)
ミドルウェアプラットフォーム事業部 所属
現在、Symfowareの開発に従事。



荒木 賢(あらかい まさる)
基盤ソフトウェア事業部第二開発部 所属
現在、AIMの開発に従事。



後藤見幸(ごとう てるゆき)
ミドルウェアプラットフォーム事業部第四開発部 所属
現在、Symfowareの開発に従事。

ま え が き

企業情報システムは、経済や社会活動と密接な関係にあり、安定稼働へのニーズが年々高まっている。とくに近年では、安定稼働の阻害要因である地震・テロなどの災害に向けた対策が急務となっている。一方、現実的には災害への対策を包括的なBCP（Business Continuity Planning）として策定している企業は少ない。その背景として、最適なソリューションがないことや、事例が少ないなどの理由が挙げられる。

本稿では、企業の生命線となるデータベースに対する最適な災害対策ソリューションとして、富士通の実績技術や新技術を生かしたSymfowareのディザスタリカバリを紹介する。

ディザスタリカバリへの要望の高まり

本章では、安定稼働の必要性と阻害要因について説明する。

企業で最優先の課題である安定稼働

現在の企業情報システムは、様々なシステムが相互に連携したサービスが行われている。このため、一部のシステム停止が多く企業、消費者に影響を及ぼす。例えば、重要なシステムが停止した場合、ビジネス機会消失という直接的な損害だけでなく、社会的信用の失墜をも引き起こすことになる。このような背景から、各企業では安定稼働が優先度の高い投資課題となってきており、中でも重要なデータを管理しているデータベースは、絶対的な安定稼働が求められる^(注1)

安定稼働を阻害する要因と対策

安定稼働の阻害要因は大きく三つあり、重要度や緊急度を見極めた最適な対策をとることが必要である。一つ目は、ヒューマンエラーやコンピュータウイルスなどの過失・故意によるトラブルである。二つ目は、ハードウェアの故障・停電などによる故障停止である。三つ目は、地震・火災・テロなどによる災害停止である。また、これらの計画外停止の要因以外にも、法定点検やソフトウェア・ハードウェア

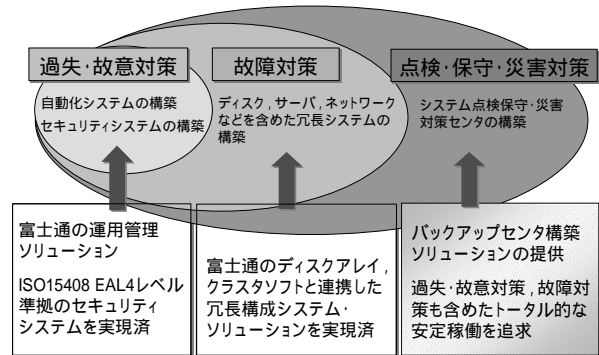


図-1 Symfowareの安定稼働への施策
Fig.1-Measures toward stable operation of Symfoware.

アのレベルアップなどの計画停止に向けた対策も重要である。

これまでSymfowareは、過失・故意や故障に対して、自動再編成などの自律化機能、秒オーダーで切替可能なクラスタ機能、セキュリティ・自動化運用などのソリューションを提供し、すでに多くのシステムに取り入れられている。これからのSymfowareは、災害対策に関しても、メインフレームの実績技術や新しいオープン技術を生かしたSymfowareディザスタリカバリを提供し、絶対的な安定稼働を実現する。

保守による計画停止などを含めたSymfowareの安定稼働に向けた施策を図-1に示す。

安定稼働に向けた取組み

本章では、災害時の安定稼働の実現方法として、センタ切替えによる業務継続とリモートセンタの構築方法を説明する。

センタ切替えによる迅速な業務再開

サイト内でのバックアップは、故障対策の最も確実な方法として従来から多く用いられているが、破壊範囲が甚大な災害を想定すると、この方法では対応できない。このため、リモートセンタに環境を復旧し、センタを切替えることで迅速に業務を再開する技術や対策が重要となっている^(注2)

これを実現するためには大きく以下の方法が考えられる。

(注1) データベースは企業情報システムの骨格となるデータを管理しており、被災により建屋が崩壊した場合などにおいても、喪失データやリカバリ時間を最小化する取組みが特に必要となる。

(注2) ニューヨークの自爆テロでは、ニュージャージーにバックアップセンタを有していたことから、即日に業務再開できたケースがあり、大きな有用性が認められている。

(1) 磁気テープをリモートサイトに搬送

データベースのバックアップデータをトラックなどで搬送し、被災時にリモートサイトのデータベースを復旧する。

(2) DBレプリケーションによるリモートサイト構築

データベースの差分ログをファイル転送などで搬送、反映することで、リモートサイトのデータベースを常に作成しておく。

(3) ストレージによるリモートサイト構築

データベースの更新結果またはデータベースそのものをストレージのリモートコピー機能でミラーリングすることで、リモートサイトのデータベースを常に作成しておく。

上記は、(1)より(2)、また(2)より(3)が、業務再開時間は短くなるがコストが大きくなる。例えば、(1)は1日分のバックアップデータをトラック搬送する場合、追加投資はわずかであるが、最大1日分のデータが消失する。さらにその復旧により業務再開時間は数日間に及ぶ。同様に(2)はファイル転送済みでない分のデータを消失し、喪失した分の復旧時間が業務再開時間に影響する。

これらのどの方法を採用するかはRTOとRPO^(注3)をどのように策定するかに依存する。つまり、指標の違いにより、とるべき手段・投資額は大きく異なる。このため、業務の重要度、緊急度を見極めたポリシーを設定することが非常に重要となる。例えば、1日分のデータ喪失が許容可能であればトラック搬送でも十分である。しかし、今日のデータベースシステムでは、絶対的な安定稼働が必要であり、本運用センタとほぼ同じデータベース環境をリモートセンタにスタンバイしておき、被災時にはセンタを切替えることで迅速な業務再開を可能とすることが必要である。センタ切替えによる迅速な業務再開を図-2に示す(以下、各センタを正センタ、副センタと呼ぶ)。

ログ SHIPPING 技術による迅速な業務再開

ストレージを利用して副センタにデータベースの複製を作成する場合、コピー対象資源により以下の

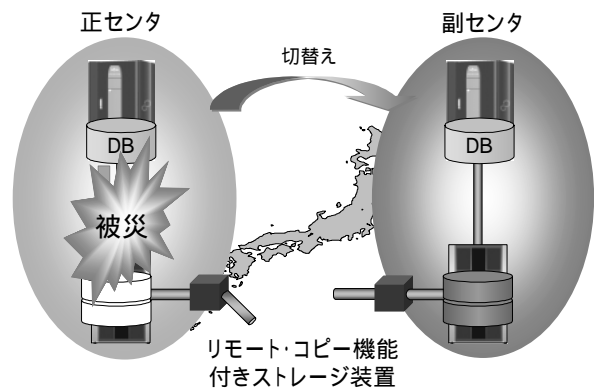


図-2 センタ切替えによる迅速な業務再開
Fig.2-Rapid resumption of business by center machine exchange.

方法がある。

(1) DBミラーリング

データベースシステム環境全体をストレージのリモートコピー対象のディスク上に配置し、正センタと副センタのデータベース全体をミラーリングする。

(2) ログ SHIPPING

データベースの差分ログファイルをストレージのリモートコピー対象のディスク上に配置し、正センタで発生した差分ログを副センタのデータベースに反映することで正センタと副センタの同値性を保証する。

なお、大規模な基幹系システムでは、転送量やデータベースの柔軟運用などにおいて、ログ SHIPPING 技術が特に有効である。

これらの方法は一般的に以下の特徴がある。

- (1) 被災時のセンタ切替え時に必要な操作として、DBミラーリングはデータベースのダウンリカバリにより状態を復元する。ログ SHIPPING は起動状態のデータベースに残存する差分ログを適用することで状態を復元する。
- (2) ログ SHIPPING は、差分ログのみコピー対象のため、コピーする量が少ない。これによりストレージ・回線のコスト削減が可能である。また差分ログはデータベースでトランザクションの整合性保証などを制御可能なため、業務保証や柔軟なセンタ運用に向いている(後述)。
- (3) DBミラーリングは単純にすべてのデータベース環境をミラーリングするため、導入が比較的容易である。

(注3) ディザスタリカバリにおいて考慮される指標として、RTOとRPOがある。RTO(Recovery Time Objective)は「どれだけ早く業務を復旧できるか」、RPO(Recovery Point Objective)は、「どれだけ前のデータに戻す必要があるか」を示す。

Symfowareディザスタリカバリの取組み

Symfowareディザスタリカバリでは、大規模システムまで含めた絶対的な安定稼働を目指している。このため、転送量の少なさやデータベースの整合性保証に優れたログシッピング方式を採用し、さらにストレージと一体となった取組みを行うことで、DBミラーリングの優位点である簡易性も目指している。本章では、前章で述べた安定稼働に向けたSymfowareディザスタリカバリの取組みについて述べる。

ストレージのミラーリング技術を利用したリアル転送

Symfowareディザスタリカバリでは、業務に対応したロググループ単位（データベースのログ環境単位）にRLP（Rerun Log Pipeline）を作成する。RLPはログの管理情報を格納するRLM（Rerun Log Management File）と、データベースの差分ログを格納する複数のRLC（Rerun Log Cycle File）で構成される。これらのファイルはリモートコピー対象のストレージ部分に配置し、リアルタイムにセンタ間でミラーリングされる。ログ環境の構成を図-3に示す。

また、正センタのデータベースを更新すると、データベースのリカバリログ取得処理の延長でログを取得し、RLCにログを書き込む。RLC内のログ量が一定量に達すると、つぎのRLCに交替してログを取得するとともに、交替が完了したRLCは副センタで読み込まれ、データベースに反映される。この仕組みによりセンタ間の等価性を維持し、常に被災時のセンタ切替えに備えている。RLC交替に

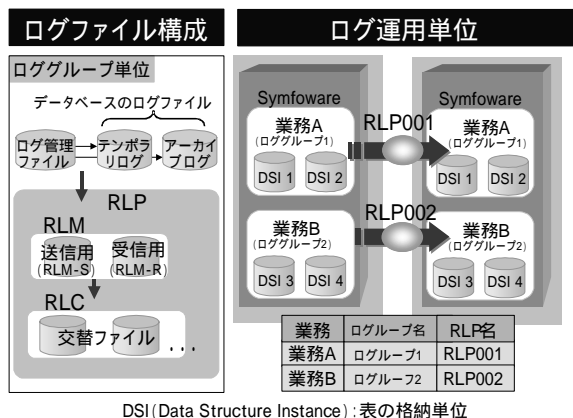


図-3 ログ環境の構成
Fig.3-Log file structure.

よるログ搬送を図-4に示す。

TCO削減

Symfowareディザスタリカバリでは、ログシッピングを採用しているため、データベースを更新した差分ログのみをコピー対象とする。さらに、独自の技術として取得する差分ログは反映に必要最小限のデータのみを対象としている（インデックスなどは取得対象外）。これにより、DBミラーリングとの比較で最大1/8にコピー対象を圧縮し、ストレージ容量や回線コストを削減する。

リカバリ範囲の削減による迅速な業務再開

ログシッピングにおいて、迅速な業務再開を行う場合、センタ切替え時の未反映のログ量を削減することが重要となる。

(1) 専用ログファイルによるセンタ切替処理の高速化

RLCの交替契機で副センタに差分ログを反映するため、センタ切替え時は、差分ログが滞留していない限り、最終のRLCに含まれる差分ログが未反映となる。このため、迅速な業務再開を目指す場合、RLCの容量が重要となる。Symfowareディザスタリカバリでは、専用のログファイルであるRLCをRTO要件に合わせて柔軟に設計することが可能である。さらに、RLCの交替契機は、動的に変更することも可能であり、計画的なセンタ切替えでは、さらに未反映の差分ログ量を少なくし、業務停止時間を短縮することが可能となる。

(2) 要件に応じた同期モード選択

Symfowareディザスタリカバリでは、トランザクション内の差分ログ書き込み保証やストレージの転送方式について、同期・非同期モードを選択できる。

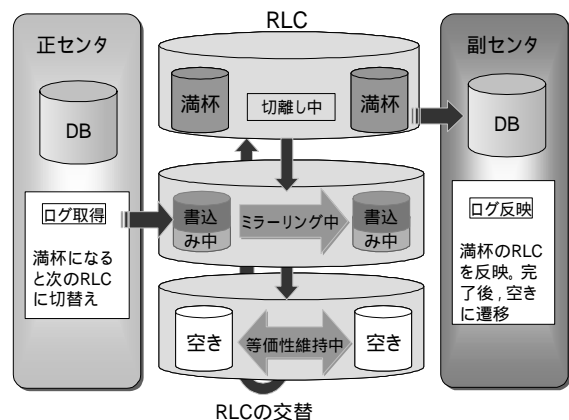


図-4 RLC交替によるログ搬送
Fig.4-Log transportation by switching RLC.

表-1 同期モードの選択

選択モード	トランザクション	ストレージ	設定方針
同期	同期	同期	データ喪失がないことを最優先する場合に設定
非同期	非同期	非同期	オンライン性能を最優先させる場合に設定

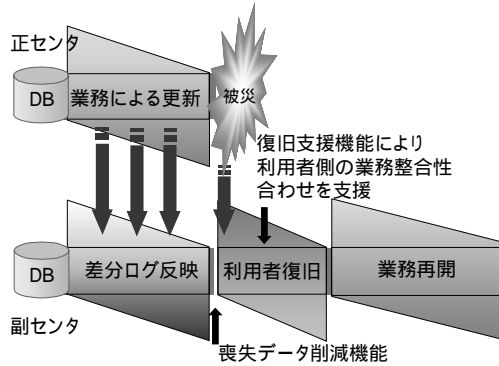


図-5 被災時の運用イメージ
Fig.5-Operation at disaster occurrence.

これにより業務性能やRTO要件に応じて、最適な設計が可能となる。

同期モードの選択について表-1に示す。

リカバリ作業軽減による迅速な業務再開

災害が発生した場合は、業務結果の到着状況調査や業務再開に向けた業務とデータベースの整合性合わせが必要となる^(注4)。これらの作業は業務との突合せが必要であり、通常容易なものではなく、いかに効率的に行うかが速やかな業務再開に向けて重要である。Symfowareディザスタリカバリは、被災時のリカバリ範囲を削減するとともに、利用者による業務整合性合わせを支援する機能により、迅速な業務再開を実現する。被災時の運用イメージを図-5に示す。

(1) 書込み中のログを最大限適用

被災時は、RLP内にデータベース未反映の差分ログが残る。Symfowareディザスタリカバリでは、喪失データ削減機能により、書込み中のRLCを含め、残存している差分ログの中から、トランザクション保証される差分ログを判断し、データベースへ反映することを可能とする。これにより、データ

(注4) Symfowareディザスタリカバリでは、トランザクション整合性は標準で保証する。業務とデータベースの整合性合わせは、フロー業務など複数のトランザクションで構成される業務で特に重要となる。

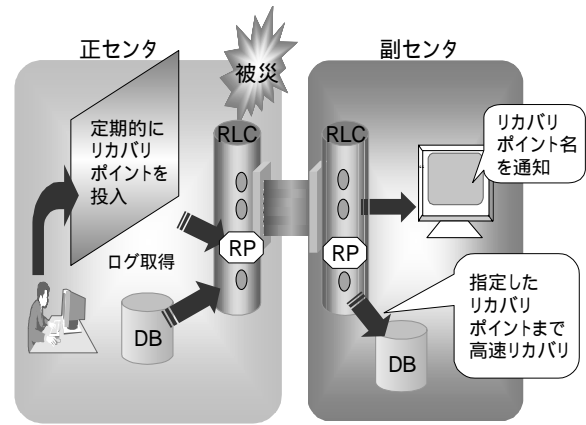


図-6 データベースリカバリ機能
Fig.6-Recovering database to recovery point using recovery function.

ベースの最新性を最大限保証したセンタ切替えを実現している。

(2) 被災支援機能による迅速な業務再開

Symfowareディザスタリカバリでは、データベースと業務の整合性合わせなどの利用者による復旧作業を支援するために、差分ログの調査機能とデータベースリカバリ機能を提供する。差分ログの調査機能は、差分ログやトランザクションの識別情報などを基に、副センタへのデータベースの更新結果の到着状況を調査することができる。データベースリカバリ機能は、通常時に正センタでリカバリポイントを定期的に投入しておくことで、被災時には選択したリカバリポイントの状態に高速に復旧することができる。データベースリカバリ機能を図-6に示す。

これらの機能は、利用者による復旧作業の効率化を実現し、実際の業務再開時間を大幅に短縮させることが可能となる。

高トラフィック業務まで保証

DBミラーリングの場合、ローカルディスクと比べてI/Oコストが高いストレージのリモートコピー対象のディスクに全データベース環境を配置する必要があり、既存の業務に影響が発生する。Symfowareディザスタリカバリでは、業務アプリケーションが直接更新対象としない専用のログファイルのみがコピー対象であり、さらに前述のコピー対象の差分ログを最大限圧縮していることからI/Oコストを削減し、既存業務を保証する。

業務への影響を最小限にしたログ取得を図-7に

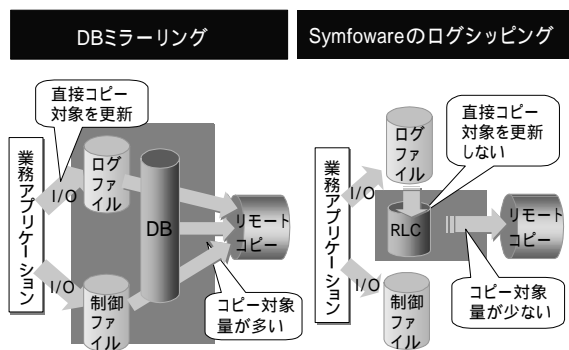


図-7 業務への影響を最小限にしたログ取得
Fig.7-Log acquisition that minimizes influence on business.

示す。

さらに、高性能ログ取得やログ反映技術により、高トラフィックでも業務に影響を与えない方式を実現している。

(1) 高性能なログ取得

非同期モードを選択した場合は、データベースのリカバリログ書込みと同様に、ログブロックを専用のI/Oキャッシュに転送するだけでログ取得が完結する。I/Oキャッシュに転送されたログブロックは、非同期で差分ログファイルに書き込むため、業務性能にはほとんど影響を与えない。

なお、ダウンが発生した場合はデータベースのダウンリカバリと連携することで差分ログの保証を行う。さらに、回線負荷などにより、バッファ枯渇などの不測の自体が発生した場合にも、ディザスタリカバリ運用だけを停止し、オンライン業務を継続させることが可能である。

(2) 高性能なログ反映

内部バスによるダイレクト反映や専用のメモリキャッシュ、負荷に応じた多重処理などの高速化技術により、正センタで発生したログを滞留なく反映する。

メインフレームの実績を生かした安定稼働に向けた取組み

オープン系の各ベンダでは、リモートコピー機能を利用した取組みを進めているが、導入している企業はまだ少なく安定稼働の面で疑問が残る。富士通は国内トップのメインフレームベンダであり、とくに金融機関など大規模なシステム構築でAIM/BKUPによる運用実績が豊富にある。以下に一例を紹介

する。

大手金融系のお客様で、約100 km離れた遠隔サイトをディスクのリモート転送によりリアルに連携し、数秒の欠損データと約2時間の業務再開時間の要件を実現した。また正センタでの保守業務時には、副センタを代替として利用するなど、バックアップセンタ構築の仕組みを有効に活用している。

Symfowareディザスタリカバリは、このような高度な要件の中で培ったAIM/BKUPの技術が生かされている。

運用性向上の取組み

Symfowareディザスタリカバリは、メインフレームでの実績に裏打ちされた確かな技術を、最新のストレージのリモートコピー機能と融合させ、運用管理の容易化などTCOを削減したバックアップセンタ構築ソリューションをオープン環境で実現する。本章では、以下に示す特徴について説明する。

- (1) ログ SHIPPINGによるセンタ切戻しによる運用性向上
- (2) ストレージ連携による両センタの運用性向上
- (3) メッセージ連携によるセンタ間業務運用連携
- (4) 論理的な反映技術によるセンタ間の柔軟性

ログ SHIPPINGによるセンタ切戻し運用性向上被災時に正センタを切り替えて業務を継続した後で、もとのセンタに切り戻して運用することができ。例えば、被災の影響がネットワーク破壊のみであった場合は、ネットワーク復旧後に、もとの正センタをいったん、副センタとして設定する。その後、センタ切戻しを行い、もとのセンタ構成に戻すことが可能となる。センタ切戻しはセンタ切替えと同様のログ SHIPPING技術で実現しており、業務停止時間は、センタ切替え時に反映が必要な差分ログを最小化する技術により、最小限に抑えることが可能になる。以下に運用イメージを示す。

- (1) 被災後に切り替えたセンタ（以下、旧副センタ）で差分ログの取得を開始しておく。
- (2) 被災したセンタ（以下、旧正センタ）が復旧した場合、データベースの状態に応じて、全件コピーまたはリカバリポイント指定のリカバリを利用することで、(1)で差分ログを取得開始した時点と同じ状態にリカバリする。
- (3) 旧副センタから復旧した旧正センタのデータ

ベースを差分ログ反映により随時反映する。この差分ログ反映中は旧副センタで業務を続けており、センタ切戻しを行うときは、最終RLCの差分ログを適用するだけでセンタ間の同値性を保証する。

ストレージ連携による両センタの運用性向上

副センタは、通常、正センタから離れた場所に設置する。しかしデータベースを常時最新化させるためには、両センタでの運用が必要となる。また長時間のネットワーク障害や他センタの電源停止などでは、他センタに影響されない独立した運用も必要となり、これらの両センタ運用にかかるコストが増大する。Symfowareディザスタリカバリでは、正センタで発生するデータベースの差分ログの状態や副センタで実施する保全データベースの最新化処理の状態をストレージのリモートコピー機能を利用し連携することで、センタ間の運用性を向上させ、TCOを削減している。

メッセージ連携によるセンタ間の業務運用連携

データベース運用の中では、構成変更や拡張などのデータベースのメンテナンスがときとして必要になることがある。このようなメンテナンスを行う際には、正センタでの実施と同期して副センタでメンテナンスを行う必要があり、タイミングを合わせるための仕組みや運用を考慮する必要がある。Symfowareディザスタリカバリでは、このような要件に向けて、センタ間のデータベース整合性を確実に保証するメッセージ連携機能を提供する。

メッセージ連携機能は、正センタで発生した運用情報を差分ログとの順序性を保証して副センタに自動通知し、必要な運用操作契機を通知する機能である。更新ログとの順序性保証は、更新ログと同様の手段でリモートコピー機能を利用してメッセージを送信することで実現する。

メッセージ連携機能を図-8に示す。

論理的な反映技術によるセンタ間の柔軟性

Symfowareディザスタリカバリでは高速に取得した差分ログを論理的に反映することで、センタ間の物理構造の柔軟性を実現している。これにより再編成運用をセンタごとに独自に行うことが可能（両センタ停止が不要）であり、柔軟性を実現している。

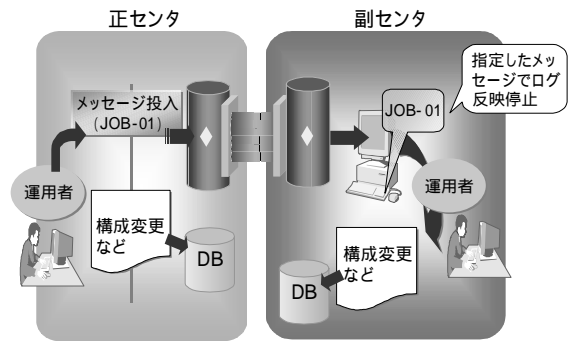


図-8 メッセージ連携機能
Fig.8-Message linkage function.

新たなソリューションへの展開

Symfowareディザスタリカバリは、副センタへのデータベース複製技術を利用して、災害対策以外のソリューションも提供する。本章では、以下について説明する。

- (1) 保守対策ソリューション
- (2) 副センタの有効利用
- (3) 静態データベース作成ソリューション
- (4) 目的に合わせた複数センタの構築

保守対策ソリューション

設備の法定点検、ハードウェア予防保守やソフトウェアのレベルアップなど、長時間を費やす保守作業においても、Symfowareディザスタリカバリのログシッピング技術を応用することで業務継続性を保証することができる。保守対策が災害対策と大きく異なるのは、センタ切替えが計画的に行えることであり、通常時は災害対策と同様に差分ログをリアルタイムにミラーリングし、副センタに蓄積された差分ログを随時反映している。センタ切替え時には、正センタのデータベースからのログ取得停止を行い、副センタで残存ログをすべて反映してから（センタ間の同値性を保証）、センタ切替えを行う。このため、喪失データは全くない。

計画切替えについて図-9に示す。

副センタの有効利用

副センタを被災時にだけ利用するのではなく、サービス拡大に向けた有効活用のニーズは非常に高い。Symfowareディザスタリカバリでは、副センタで参照業務を実行可能であり、日中は正センタでオンライン業務を実行し、夜間は参照業務向けに副

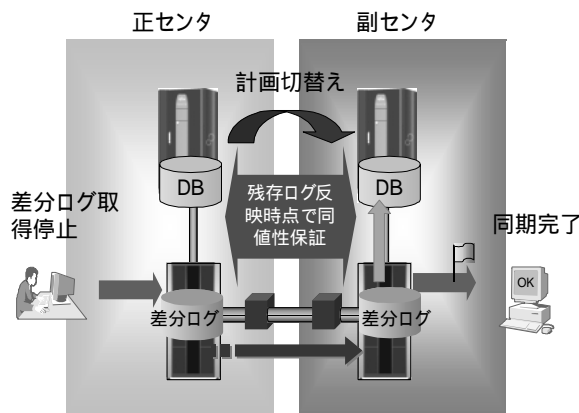


図-9 計画切替え

Fig.9-Center machine is switched in advance.

センタを利用するなどの有効活用が可能である。

なお、他社のログ SHIPPING では、副センタで参照業務を実行するために、データベース再起動や、コストの高いログ取得・反映処理が必要である。Symfowareディザスタリカバリでは、高速に取得した差分ログを論理的に反映する技術により、副センタで常に参照業務として利用可能である。

静態データベース作成ソリューション

金融系システムなどでは、日々の運用の中で利盛処理（利息付与）などのバッチ処理が必要である。このとき、オンライン業務への負荷を考慮して、別サーバにデータベースの静止状態を作成してバッチ処理を実行する方法がよく用いられる。Symfowareディザスタリカバリでは、ログ SHIPPING 技術を応用することで、副センタをバッチ用サーバとして利用可能である。副センタでの静止状態のデータベース作成を図-10に示す。

- (1) 正センタで静止状態が必要なタイミングで凍結ポイントを投入する。このとき、投入した凍結ポイントは自動的に副センタに伝播する。
- (2) 伝播された凍結ポイントの地点で差分ログの反映を自動的に停止し、バッチ処理開始可能を示すメッセージを出力する（静止状態の作成完了）。

目的に合わせた複数センタの構築

絶対的な安定稼働が求められる災害対策を行う場合には、3重、4重の副センタ設置が必要な場合がある。Symfowareディザスタリカバリでは、一つの正センタに対し、副センタを複数構築することができる。また、複数の副センタは災害対策の目的だ

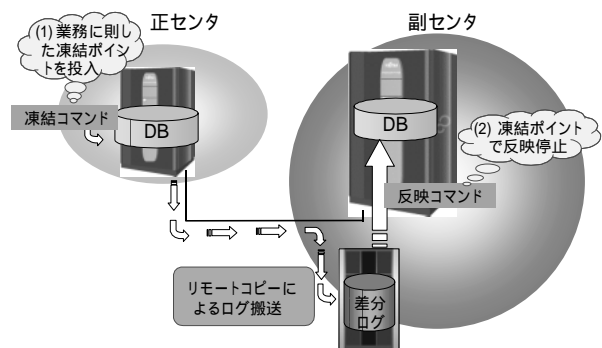


図-10 副センタでの静止状態のデータベース作成
Fig.10-Snapshot of database is made for standby center.

けでなく、保守対策やバッチ業務として利用することもできる。このため、万が一の備えとしてだけでなく、目的別に副センタを有効活用することも可能となる。

む す び

Symfowareは、お客様にゆるぎない安心を提供する高信頼なデータベースとして、比類なき安定稼働と省力運用を開発目標とし、徹底したものづくりを行っている。例えば、安定稼働に向けては、秒オーダーの高速切替やスケールアウトを実現するクラスタシステム、瞬時バックアップ機能や世界最高速の性能などを含め、豊富な稼働実績を残している。また、省力運用では、自動再編成機能などの自律化技術やグリッド技術を駆使した自動化をはじめ、トータルに使いやすいデータベース環境を実現している。さらに長期保証を行い、数多くのお客様から評価されている。

Symfowareディザスタリカバリは、これらSymfowareの高信頼性技術とメインフレームの実績技術、さらにハードウェア新技術などの富士通のコアコンピタンスを集結し、ハイエンドまで対応可能なバックアップセンタ構築による絶対的な安定稼働を実現する。

さらに、保守対策や静態データベース構築などの有効利用やストレージと一体となった運用機能など、IT基盤「TRIOLE」技術との相乗効果による省力運用を実現し、今日のグローバルな企業経営において、ハイレベルなビジネスコンティニュティを実現する。