



ディザスタリカバリなどBCP対策にも

ハイブリッドクラウドが 有効な選択肢に

自然災害が多発する日本。
企業に適したデータ保護とビジネス継続対策とは

ビジネス継続性とデータ保護を支える上での重要な技術的な要素、予防措置となっているのがディザスタリカバリです。特に日本では、自然災害リスクへの対策と法的要件への対応の両面から、その重要性が高まっています。そうしたディザスタリカバリの実現に向けて、システム運用の柔軟性と高度な信頼性を最適なコストで提供する有力な解決策の1つとして注目されているのが、ハイブリッドクラウドの活用です。

ビジネス停止のリスクを回避するディザスタリカバリとは？

デジタルトランスフォーメーション（DX）が進む中、今やあらゆる企業のビジネスがITシステムを前提に運用されていると過言ではありません。そのため、システムに発生した計画外のダウンは、そのままビジネス停止に直結することになります。

そのような際に求められるのがディザスタリカバリ（災害復旧）です。システムがダウンする要因は地震や津波、台風などの自然災害だけに限りません。システムに潜んでいた不具合やプログラム改修の影響など技術的な障害、ソフトウェアのバージョンアップに伴う非互換性の顕在化、単純なヒューマンエラー、サイバー攻撃などさまざまな要因によってシステムはダウンする可能性があります。

これらの多岐にわたるリスクを考慮した上で、緊急事態が発生した際にシステムやデータの継続的な保護とスムーズな復旧を図るための戦略と手法、そしてそれを具現化した仕組みを総称したものがディザスタリカバリです。

その意味でもディザスタリカバリは、ITに限った課題ではなく経営課題であることをしっかり認識しておく必要があります。重要なデータの喪失やビジネスプロセスの停止を防ぎ、ひいては顧客の信頼性を確保して自社の損害を最小限に抑えるためにもディザスタリカバリは不可欠であり、BCP（事業継続計画）対策の柱となります。

ディザスタリカバリなどBCP対策にも
ハイブリッドクラウドが有効な選択肢に

自然災害が多い日本ではディザスタリカバリが必要不可欠

日本は地震、津波、台風などの自然災害のリスクが非常に高い国であるため、特にディザスタリカバリが必要とされます。実際、日本でディザスタリカバリが注目されたきっかけは、2011年3月11日に起こった東日本大震災にあったとされています。

総務省の「情報通信白書 平成24年版」^{※1}には、同震災の被災地において実施したインタビュー調査の結果が示されており、これによればデータ損失の被害を受けた企業や自治体は、全体の33.1%（自治体30.0%、企業25.8%、その他40.0%）に達しています。また業務システムの被害については全体で36.8%となっています。この経験が大きな教訓となり、ディザスタリカバリを導入する企業が全国に拡大して

いきました。

さらに昨今、企業がビジネスを行う上で重要な役割を果たすデータの保護と事業の継続性は、法的要件や顧客への責任といった観点からも重要な課題となっています。例えば、顧客のプライバシーに関するデータは、ディザスタリカバリにおいても個人情報保護法に則った形で保護や復旧が必要です。また、法人顧客からは契約に際して、ディザスタリカバリに関連してポリシーや実施手順、互いの責任範囲などを明記した法的文書を求められる場合もあります。

このようにディザスタリカバリは万一の事態に備えた対策としてだけではなく、平時のビジネスを行う上でも必須の施策となりつつあります。

※1 総務省「情報通信白書 平成24年版」

業務継続性確保で押さえるべき3つの要件

ディザスタリカバリを実現する手段としては、システムのバックアップデータを遠隔地に送って保管する方法や、ネットワークを経由して遠隔地の拠点からリモートバックアップを取る方法などがあります。加えて、より高度な業務継続性を確保するためには、以下の3つの要件を考慮する必要があります。

① RTO (Recovery Time Objective : 目標復旧時間)

システムを復旧して業務を再開するまでに要する時間。当然のことながら短ければ短いほどよいとされます。

② RPO (Recovery Point Objective : 目標復旧時点)

障害発生後、どの時点までのデータを復旧させるのかを示したもので、業務内容によって求められる値が違ってきます。更新頻度の低いシステムは、システムダウンの前日までのデータが復旧できれば

業務に大きな支障は生じないかもしれませんが、金融機関の勘定系のようなシステムでは、ダウンの直前まで行われていた取引のトランザクションデータを漏れなく復旧させる必要があります。

③ RLO (Recovery Level Objective : 目標復旧レベル)

どのレベルまでシステムを復旧させるのかを示した値で、例えば「災害発生前の50%以上のユーザーが利用できる状態まで復旧する」といった目標を設定します。

RTOやRPOを可能な限り最小化しつつ、RLOを最大化するためには、現在のデータセンター（本番サイト）から地理的に離れた場所にバックアップ用のデータセンター（代替サイト）を用意し、この2つのサイト間で同期をとりながらデータのレプリケーション（複製すること）をリアルタイムに近い形で行います。



これなら本番サイトが被災してシステムの続行が不可能となった場合でも、代替サイトに運用を切り替えることで、迅速に業務を再開することができます。

ただし、この方法はコストを要するため、企業規模や使える予算によっては実現が難しいことがあります。代替サイト用のデータセンターを新たに確保し、

本番サイトと同等のハードウェアやソフトウェア環境を代替用のデータセンターにも用意するとなれば、システムの所有・運用コストは単純計算で2倍になってしまいます。限られたIT予算の中で、万が一の非常事態に備えるためだけに、そのような投資を行える企業は多くありません。

ディザスタリカバリ実現にはハイブリッドクラウドという選択肢

ここで注目されているのが、ハイブリッドクラウドの活用です。ハイブリッドクラウドとは、クラウド事業者がサービスとして提供しているパブリッククラウドと、企業のオンプレミス環境に構築されたシステム（プライベートクラウドを含む）を適材適所で組み合わせて運用するアーキテクチャーです。

パブリッククラウドはハードウェアやOSを保持する必要がなく、動的に拡大縮小できます。オンプレミ

スも最近ではサブスクリプション型（as a Service型）にてインフラを利用できるサービスが提供されています。これらを組み合わせれば業務要件に応じたバックアップやレプリケーションを行うことが可能となり、最適なコストで障害や災害発生時にデータやシステムの継続的な可用性を確保し、ひいては高度な業務継続性を実現することができます。

ハイブリッドクラウドにおけるディザスタリカバリの構成

パブリッククラウド上に代替サイトを構築した場合も、本番サイトと同等のリソースを用意する必要がありますが、平時にはアプリケーション実行に用いる仮想サーバーなどのリソースの電源をOFFにすることにより、無駄なコストの発生を避けることができます。このような仕組みもハイブリッドクラウドを活用したディザスタリカバリのメリットです。

代替サイトに本番サイトと同等のシステムを準備し、システムの双方のストレージ間でデータのレプリケーションを行っておけば、本番サイトがダウンした際に、代替サイト側で待機させていた仮想サーバーの電源をONにするだけで、短時間でシステムを再開することができます。

さらにパブリッククラウドの代替サイト上で稼働するシステムは、インターネットに接続できる環境さえあ

れば、どこからでも簡単にアクセスすることが可能です。災害発生時に、社員が在宅勤務や遠隔地のサテライトオフィス勤務などに切り替えた場合でも、スムーズにシステムを利用して業務を再開することができます。これは前述したRLOを最大化するためにも大きな効果があります。

ただし、ハイブリッドクラウドを活用したディザスタリカバリを構築する際にも、留意点があります。それはストレージに関する問題です。パブリッククラウド上で利用するストレージは、単にデータのレプリケーションに耐えられる容量さえ確保しておけばよいわけではありません。本番サイトで利用しているストレージと同等の信頼性とパフォーマンスを備えていることが条件となります。

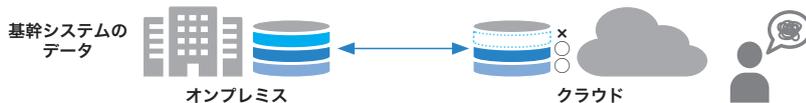
代替サイトで調達したクラウドストレージが十分な信

ディザスタリカバリなどBCP対策にも
ハイブリッドクラウドが有効な選択肢に

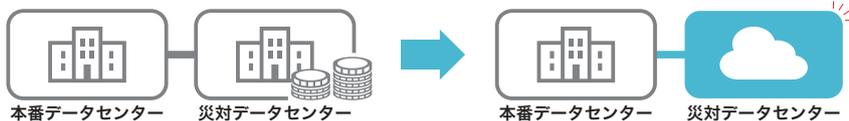
ハイブリッドクラウドではデータのサイロ化が生じる恐れもあるので、オンプレミスとクラウド間の確実なデータ連携が重要となる

クラウド活用における課題

- 基幹システムの持つデータを取り扱うにあたり、オンプレミスとクラウド間では、確実なデータ連携が必要



- データセンターファシリティの維持にコストがかかる→利用頻度の低い災害環境をクラウド化したい



信頼性を備えていなかった場合、本番サイトと間のデータのレプリケーションが正確に行われず、パフォーマンスが劣る場合も同様で、同期スピードに追いつけず、データの漏れや破損が発生してしまうおそれがあります。本番サイトと代替サイトの間で同じデータを保持しているという大前提が崩れて不整合が生じてしまい、ディザスタリカバリは成り立ちません。

また本番サイトのストレージと代替サイトのストレージの間で、構成や機能面などの仕様が異なるのも大きな問題となります。双方でそれぞれ異なるメンテナンスやデータ管理を行わなければならないためです。ストレージの運用管理の手間が二重化し、ハイブリッドクラウドの本来の特徴である運用の省力化や、コス

ト最適化といったメリットが失われてしまいます。

こうした条件を考慮した上でお勧めしておきたいのは、本番サイトと代替サイトの間で共通のアーキテクチャーをもったストレージを利用することです。信頼性やパフォーマンスに優れ、同じ仕様に基づいて利用できるストレージを、オンプレミスのシステムとパブリッククラウドの双方に配置して組み合わせることで、より安心で確実性の高いデータやアプリケーションのバックアップ、レプリケーションならびに復元が可能となります。さらに高度なストレージ機能によって自動化されたデータのバックアップとレプリケーションは、リアルタイムでのデータ保護を実現し、可用性の向上に貢献します。

ディザスタリカバリはリスクを抑え継続的な成長と競争力強化に必要不可欠

先述してきたようにディザスタリカバリは万一の非常事態に備えた対策としてだけではなく、平時のビジネスを行う上でも必須の施策となりつつあります。また、自社の業務要件やシステムの重要度に合わせて、RTO（目標復旧時間）、RPO（目標復旧時点）、RLO（目標復旧レベル）の3つの目標を考慮した、ビジネス継続とデータ保護の仕組みを整えておくべきです。

そうしたディザスタリカバリを最適なコストで実現し、効率的に運用していく手段としてハイブリッドクラウドの活用が有効です。ここで特にお勧めしておきたいのは、本番サイトと代替サイトの間で共通のアーキテクチャーをもったストレージを利用することです。信頼性やパ

フォーマンスに優れ、同じ仕様に基づいて利用できるストレージをオンプレミスのシステムとパブリッククラウドの双方に配置して組み合わせることで、同じような設計・運用で負担が減らせるだけではなく、より安心で確実性の高いデータやアプリケーションのバックアップ、レプリケーションならびに復元が可能となります。

このようにハイブリッドクラウドは、ディザスタリカバリにおいて柔軟性と信頼性を提供する解決策の有力な選択肢となります。顧客の信頼性を高め、リスクを最小限に抑え、継続的な成長と競争力を確保するためにも、一日も早く手を打っていただければと思います。



ディザスタリカバリなどBCP対策にもハイブリッドクラウドが有効な選択肢にも

ハイブリッドクラウドで実現するデータ保護のイメージ

DRで実績のあるストレージコピーをクラウドにも適用、利用頻度の低い災対環境をクラウド化 SoR(基幹業務DB)データの分析環境をハイブリッドクラウドで構築

ハイブリッドクラウドでのDR環境構築時のニーズ例

- 利用頻度の低い災対環境をクラウド化したいがオンプレミスとの同期や構成設計が難しい
- 災対環境として維持しておくだけでなく、分析環境としてクラウド上で活用したい

メリットと利用シーン

- エンタープライズ環境のDRで実績のあるストレージコピーをクラウドにも適用、利用頻度の低い災対環境のクラウド化を実現→ストレージ間で同期することで代替サイトのリソースを一部電源OFF、コストを最適化
- クラウド上のBIツールやクエリサービスから分析を実行

