

特別企画

ビジネスの継続性を保証するNTT Comの グローバル・ディザスタ・リカバリ・ソリューション

グローバルIPソリューションカンパニーとして、世界規模で幅広いIPソリューションを展開するNTTコミュニケーションズ。同社では2003年2月に、世界で初めて日米間を結ぶデータバックアップシステムを構築した。これにより、災害やウィルスなどでITシステムに被害を受けても、顧客情報や財務情報などの大切な企業データは保護され、ネットワーク経由で速やかにITシステムを復旧させることが可能となった。

ビジネスを決してストップさせないための危機管理ソリューション。それが、NTTコミュニケーションズの「グローバル・ディザスタ・リカバリ・ソリューション」である。(編集部)



NTTコミュニケーションズ(株)
ITマネジメントサービス事業部
カスタマーサービス部長
NPO日本ネットワーク
セキュリティ協会理事
工学博士
松尾 直樹氏



NTTコミュニケーションズ(株)
ITマネジメントサービス事業部
カスタマーサービス部
プロセスインフラ部門
グローバルプラットフォームサービスPT
担当課長
馬場 登志郎氏

第1章 グローバルビジネスに不可欠な災害対策
(DR ; Disaster Recovery)

第2章 ビジネスの継続性を保証するGDRソリューション

第3章 GDRソリューションの導入事例と高付加価値
サービスの展開へ向けた取組み

第1章

グローバルビジネスに不可欠な 災害対策 (DR ; Disaster Recovery)

企業の活動に不可欠なデータやシステムを不測の事態から守る「ディザスタ・リカバリ(DR)」の重要性が高まっている。特にビジネスをグローバルに展開する企業にとっては、グローバルな視野でのビジネスの継続性 (Business Continuity) を高めるDR対策は必要不可欠だ。本章では、こうしたビジネス環境におけるDR対策の重要性とポイントについて述べる。

リスクマネジメントの観点で、 ますます高まる DR の重要性

企業の活動がIT (情報技術) に大きく依存するようになった現在、システムの障害や停止は、即業務の停滞につながると同時に、顧客や取引先との信頼関係に影響を及ぼしたり、社会的な信用問題にも発展しかねない。企業にとって情報 (データ) は重要な資産であり、システムの継続運用は企業活動の生命線である。このような企業活動の重要な基盤を担う情報通信システムの継続的な運用と迅速な復旧のために、不測の事態に備える「DR (ディザスタ・リカバリ)」が注目を集めている。

災害によるシステム障害の例として、日本では特に、地震によるシステム障害が考えられる。例えば1994年に起きた阪神淡路大震災での情報通信システムのハード・ソフト資産の被害件数は莫大な数にのぼった。またニューヨークでは、2001年の同時多発テロや、2003年はじめに起きた大規模かつ広域なBLACK OUT (停電) によって、

莫大な経済損失が発生した。その他最近では、中国を中心に猛威をふるったSARSによって、要員がビル内に入れなくなってしまったためにシステムの運用・操作が出来なくなったというこれまでにない災害事例もでてきている。このように、災害対策の対象は、テロ攻撃やハッキング、サイバーテロ、データの漏洩といった人為的なものから、地震、洪水、停電、SARSなど、広範囲に及んで

いる。人為・自然災害による不測の事態が発生した場合、いかにデータを守り、ビジネスの継続性 (Business Continuity) を維持するかが、リスクマネジメントの観点から極めて重要である。

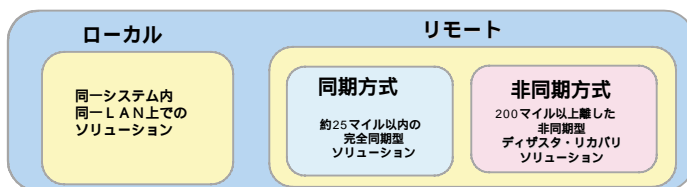
2001年9月のニューヨークを襲った同時多発テロでは、多くの企業が情報通信システムとともに顧客データなどの重要な経営資源を失うことになったが、DR対策を講じてい

ディザスタ・リカバリ (DR) とは

ディザスタ・リカバリ (DR) とは、直訳すると「災害からの復旧」ということであるが、災害 (自然災害・人為災害) に起因するシステム障害の影響を最小限に抑えるために、普段から代替システムやバックアップ・データを用意しておくシステム運用体制を指している。米国の『金融システムの安定性強化に向けた着実な実践』という白書の中では、DR代替施設は、200マイル (約320km) 以上隔離した立地での実現が推奨されている。

バックアップ方法として、ローカル、つまり同一システム内、同一LAN内では、システムバックアップやテープバックアップなどが利用される。リモートの場合は、同期型と非同期型のバックアップ方法があり、25マイル以内の場合ではデータの整合性を完全に取ることが可能な同期型が利用される。200マイル以上離す必要がある場合、現在の技術ではリアルタイムバックアップは課題があるため、非同期型技術が適用できる。従ってDRソリューションにはリモートバックアップの非同期型方式が採用されることになる。

バックアップ方法



た企業だけは、早期復旧が実現できたとされている。この教訓を踏まえ、『米国金融システムの安全性強化に向けた着実な実践』白書の中でも、「バックアップを行わずに失った障害は、システム管理者、ひいては経営者の責任である。」と明記するなど、DR対策の必要性が強調されている。

リスクマネジメントの欠如がもたらす莫大なダウンタイムコスト

ビジネスの継続性に対するリスクマネジメントを怠ると、企業は多大な損失を被ることになる。システム障害が起こると、当然それに伴うダウンタイムコストが発生する。製造ラインや営業活動の停止による利益損失だけでなく、売上・顧客情報、財務情報など大切な企業情報の消滅、損害賠償請求の補償など莫大な損失が発生する。またシステムの復旧に要するコスト（人、時間、機会費用）も発生する。さらに、ビジネスの停止による企業価値や企業イメージの低下など間接的に発生する損失も考えられる。

米国の調査会社 Contingency Planning Research & Strategic Research Corp. から出ているダウンタイムコストの一例を図1に示す。この図は、1時間あたりのダウンタイムコストを示したものである。例えば金融機関の場合、1時間あたり650万ドル（約7億200万円）の損失があるとされている。なお、これらのデータは1時間あたりのダウンタイムコストであるので、もし

ニューヨークで起きた大規模停電のように復旧まで30時間以上かかった場合には、この30倍の被害が発生すると予測される。

このように、災害などによるシステム障害は、起こる確率はそれほど高くはないが、起きた場合の損害は非常に大きいといえる。

ディザスタ・リカバリの指標と注目され始めたDRソリューション

ディザスタ・リカバリの基本的な考え方は、システム障害によるダウンタイムを限りなくゼロに近づけることである。しかし、堅牢なDR環境を構築するためには莫大なコストが必要になる。従ってDR対策のレベルに応じて必要なコストも変わってくる。企業は、投資コストと災害時の損失コストを勘案したうえで、自社のニーズに最適なDR環境を構築することが重要である。

対策レベルの目安となるのが、「RPO」と「RTO」の2つの指標である。RPO（Recovery Point Objective）は、災害の後ビジネスを再開するのに、どの時点までのデータをリカバリする必要があるのか、言い換えれば災害発生からどのくらい前のデータを保存しておく必要があるかの指標である。また、RTO（Recovery Time Objective）

金融機関および商取引が発生する業種では、ダウンタイムによる損失が大きい

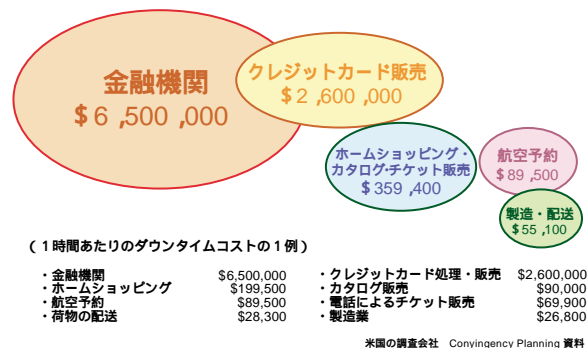


図1 ダウンタイムコストの例

は、災害の後、ビジネスを再開するために、必要なデータがリカバリされるまでの経過時間はどのくらいか、言い換えればどのくらいの時間でデータを復旧できるかの指標である。企業は「Business Continuity Plan」（以下、BCP）を全社方針として策定し、各情報システムの要求条件に沿ったRPO・RTOを実現しうるDRソリューションを選択する必要がある。図2に、基本的なディザスタ・リカバリを実現するソリューションの例を示す。ディザスタ・リカバリ・ソリューションは大きく2つの方法に分類出来る。1つ目の方式は、データのみバックアップを行うDR方式である。この方式には定期的に遠隔地にデータをバックアップする方式と、差分が発生したら順次レプリケーションする方式がある。これらの方式は災害発生後プライマリサイトのアプリケーションを復旧した後、リモートサイトのバックアップデータからリストアをかけてシステムを復旧させるものである。2つ目の方式は、アプリケーションを含むバックアップを行うDR

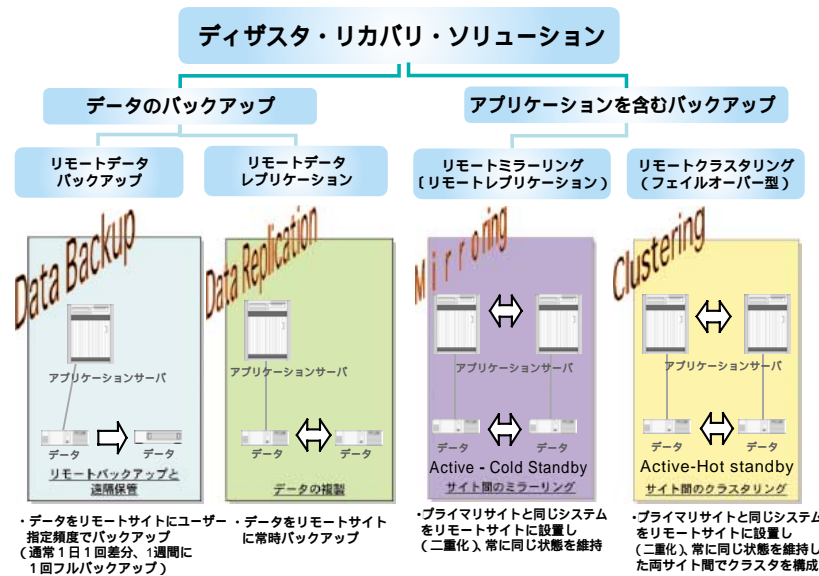


図2 ディザスタ・リカバリを実現するソリューション

方式である。この方式はリモートサイトにもアプリケーションを用意し災害発生時にはリモートサイトで運用する方式である。コールドスタンバイのリモートミラーリング方式とホットスタンバイのリモートクラスタリング方式がある。

ディザスタ・リカバリ環境の構築には、サーバ、データベース、ストレージ、ネットワークなどの広範囲な知識やシステム構築ノウハウが必要であるし、24時間365日の運用・管理体制を確立する必要がある。しかしその全てを自社の情報システム部門で実現することは、なかなか困難である。このような課題を解決するためには、24時間365日体制によるリモート監視やシステムの管理・運用までを専門家集団にアウトソースする方法がある。プロバイダが提供するサービスの利用は、要員の確保や新技術の導入といった面も含めて企業にとって極めて有効な手段である。

グローバルな視点でのリスクマネジメントが不可欠

グローバルにビジネスを展開する企業にとって、ビジネスの拠点が海外各地に散在しているということもあって、不測の事態に遭遇する機会も多い。海外に製造拠点を持つ企業にも同様のことがいえる。通常、そのような企業では拠点（国ないし地域）単位でディザスタ・リカバリ環境を構築しているのが現状である。企業活動のグローバル化が進展している現在、情報やデータを共有する必要があるだけでなく、そのディザスタ・リカバリ方針もグローバルな視点で統一していく必要がある。

このようなニーズに対応して、NTTコミュニケーションズ（以下、

NTT Com）では、「GDR（グローバル・ディザスタ・リカバリ）ソリューション」を提供している。GDRソリューションは、その名のとおりに、グローバルな視点でディザスタ・リカバリを行う環境を提供するサービスである。

グローバルなDRが必要とされる理由としては、ビジネスのグローバル化や、日系企業における海外依存度（海外売上比率）の高さがあげられる。一例として、図3に、精密機器業と自動車業の海外依存度を示す。例えば精密機器業では、海外依存度70%以上の企業が46%も存在する。このようなビジネス環境においては、国内外に分散しているITリソースを統合し、コスト削減を図り、経営資源を一元的に管理していくとともに、グローバルな視点でリスクマネジメントを行う必要があるといえる。

こうしたシステム障害による莫大な損失を防ぎ、ビジネスの継続性を確保するための有効な手段となるのが、NTT Comが提供するGDRソリューションである。

次章では、こうしたニーズに応えるNTT ComのGDRソリューションについて詳しく紹介する。

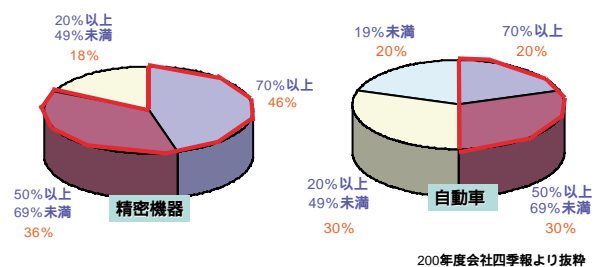


図3 日系企業における海外依存度